IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

SHINGLETOP IP LLC, Plaintiff, v. ACER INC. and ACER AMERICA CORPORATION, Defendants.	Civil Action No. 6:21-cv-861 **Jury Trial Demanded**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Shingletop IP LLC ("Shingletop") files this Complaint against Acer Inc. and Acer America Corporation (individually and collectively referred to herein as "ACER" or "Defendant") for patent infringement of United States Patent Nos. 8,185,156; 8,467,831; and 9,532,208 (the "patents-in-suit") and alleges as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

THE PARTIES

2. Plaintiff Shingletop IP LLC is a Texas limited liability company with a principal place of business located at 9901 Brodie Lane, Suite 160-934, Austin, Texas, 78748.

3. On information and belief, Defendant Acer Inc. is a corporation organized and existing under the laws of Taiwan that maintains an established place of business at 1F, 88, Sec. 1, Xintai 5th Road, Xizhi, New Taipei City 221, Taiwan.

4. On information and belief, Defendant Acer America Corporation is a corporation organized and existing under the laws of the State of California having a primary place of business located at 1730 North First Street, Suite 400, San Jose, CA 95112. On information and belief, Defendant Acer America Corporation has transacted and continues to transact business in the State of Texas under Texas Taxpayer Number 17700277365. On information and belief, Defendant Acer America Corporation may be served with process through its registered agent, CT Corp. System, located at 1999 Bryan St., Ste. 900, Dallas, Texas 75201.

5. On information and belief, Acer, directly or indirectly imports, sells, and offers to sell computers in the United States, including in the Western District of Texas.

6. On information and belief, Acer, directly or indirectly owns and/or operates a regular and established place of business within the Western District of Texas located at 1394 Eberhardt Road, Temple, Texas, 96504.

7. On information and belief, Acer infringes the patent-in-suit by at least making, selling, offering for sale, and/or importing, without authorization, Shingletop's proprietary technologies as contained in a number of Acer's commercial products including, *inter alia,* laptops and mobile devices branded with the Acer trademark;

laptops and mobile devices incorporating eSIM technology;[1] laptops and mobile devices incorporating Gemalto eSIM technology;[2] laptops and mobile devices incorporating Thales Group eSIM technology;[3] laptops and mobile devices having pre-installed eSIM data plans;[4] laptops and mobile devices having pre-installed Ubigi eSIM data plans;[5] model Swift 3 laptops;[6] model Swift 7 laptops;[7] model TravelMate P2 laptops;[8] model TravelMate Spin P4 laptops;[9] model TravelMate P6 laptops;[10] model Spin 7 laptops;[11] and other laptops and mobile devices which function in a substantially similar way to

[1] *See* https://www.usmobile.com/blog/list-of-esim-compatible-devices/.

[2] *See* https://www.businesswire.com/news/home/20180530005103/en/Want-to-Have-4G-Connectivity-on-your-PC-Everywhere-you-go-With-Acer-and-Gemalto-you-can.

[3] *See* https://www.thalesgroup.com/en/markets/digital-identity-and-security. (re-directed from www.gemalto.com).

[4] *See* https://cellulardata.ubigi.com/.

[5] *See* https://cellulardata.ubigi.com/help-center/faq/esim-data-plan/which-mobile-devices-support-ubigi-esim-windows-10-laptops/.

[6] *See* https://www.acer.com/ac/en/US/content/4g-lte.

[7] *See* https://www.acer.com/ac/en/US/content/4g-lte.

[8] *See* https://www.esim.net/helpdesk/laptops-with-esim/.

[9] *See* https://www.acer.com/ac/en/US/content/professional-series/travelmatespinp4.

[10] *See* https://www.acer.com/ac/en/US/content/professional-series/travelmatep6.

[11] *See* https://cellulardata.ubigi.com/help-center/faq/esim-data-plan/which-mobile-devices-support-ubigi-esim-windows-10-laptops/.

the previously specified laptops and mobile devices. (Collectively and individually referred to herein as the "Accused eSIM Products.")

SUBJECT MATTER JURISDICTION

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 et seq.

JURISDICTION AND VENUE AS TO DEFENDANT ACER INC.

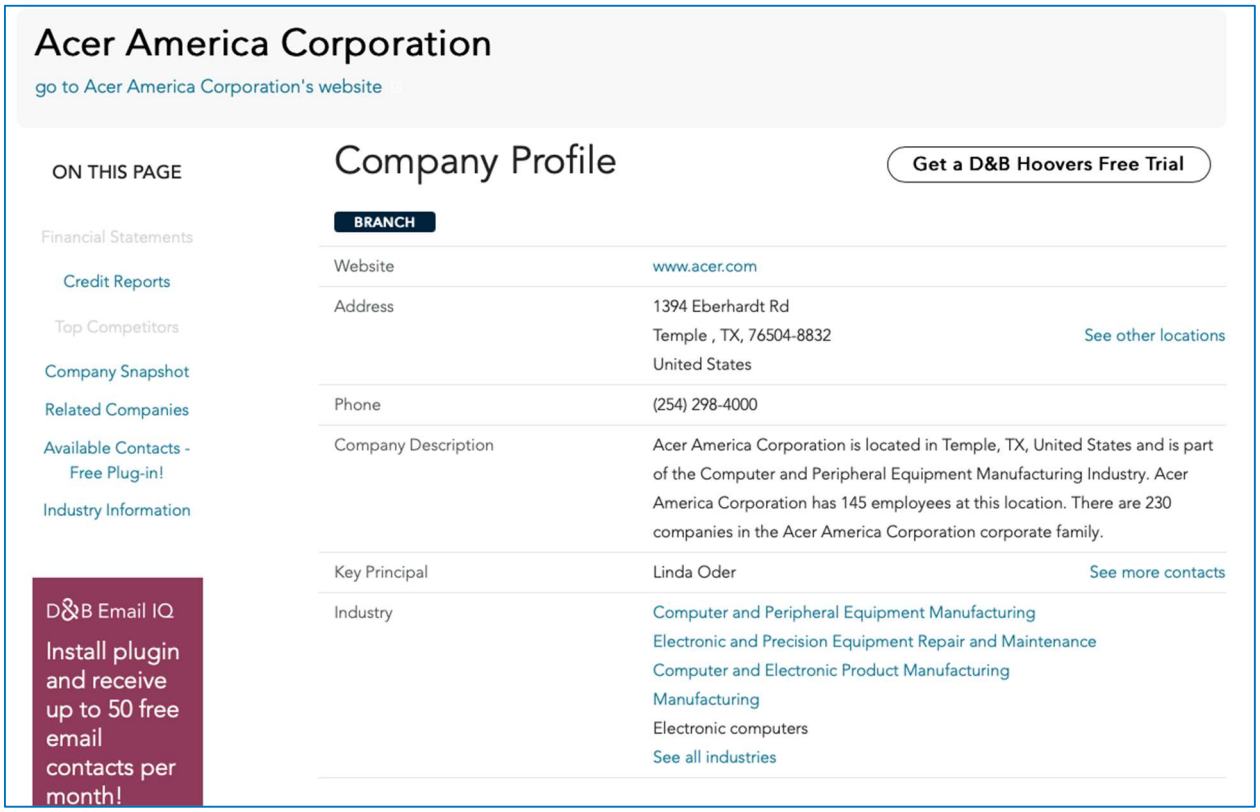
9. Defendant Acer Inc. is subject to personal jurisdiction in the United States, and specifically in Texas, pursuant to Fed. R. Civ. P. 4(k)(2).

10. On information and belief, Acer Inc. is not subject to jurisdiction in any state's courts of general jurisdiction. Acer Inc. has sufficient minimum contacts with the United States that include, *inter alia*, importing, advertising, offering to sell, and/or selling the Accused eSIM Products throughout the United States, including in the State of Texas and this judicial district, and such that Acer Inc. should reasonably and fairly anticipate being hauled into court in the State of Texas and this judicial district.

11. This Court has personal jurisdiction over Defendant Acer Inc. because it committed and continues to commit acts of infringement in this judicial district in violation of 35 U.S.C. § 271(a). In particular, on information and belief, Acer Inc. has made, used, offered to sell, and/or sold the Accused eSIM Products in the Western District of Texas.

12. This Court has personal jurisdiction over Acer Inc. pursuant to the Texas Long Arm Statute. See Tex. Civ. Prac. & Rem. Code §§ 17.042(1), (2), and (3).

13. On information and belief, Defendant Acer Inc. recruits Texas residents, directly or through an intermediary located in this state, for employment inside or outside this state.



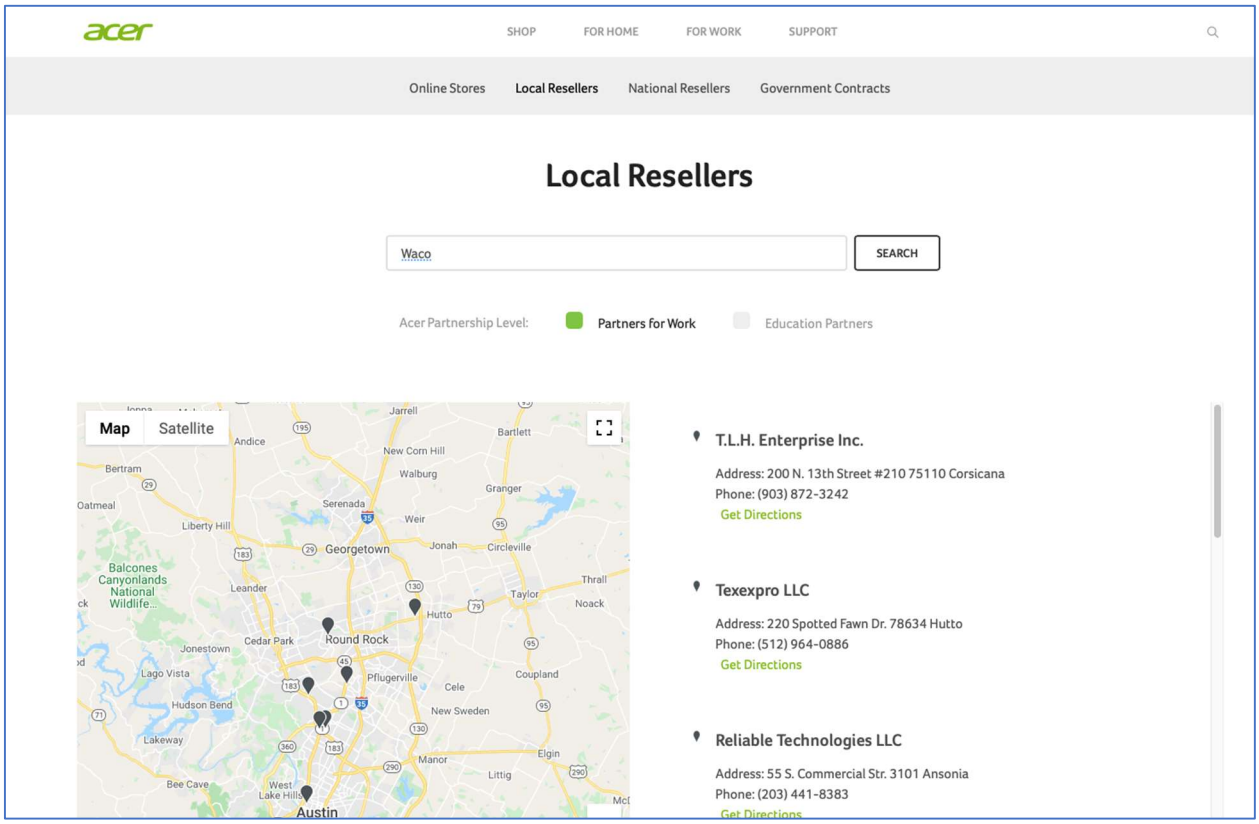
See https://www.dnb.com/business-directory/company-profiles.acer_america_corporation.5f8d9d3b820c909931a31ca1fcfb8403.html.

14. On information and belief, Acer Inc. either directly or indirectly employs at least 145 Texas citizens in this judicial district. *See* Id.

15. On information and belief, Defendant Acer Inc. is subject to the Court's personal jurisdiction because it regularly conducts and solicits business, or otherwise engages in other persistent courses of conduct in the State of Texas and in this judicial district, and/or derives substantial revenue from the importation, sale, and distribution

of goods and services, including but not limited to the Accused eSIM Products, to individuals and businesses in the State of Texas and in the Western District of Texas.

16. On information and belief, Acer Inc. has purposefully directed its marketing, sales, distribution, and importation activities towards, and in relation to, the State of Texas and its residents.



See e.g. https://www.acer.com/ac/en/US/content/series/swift7; https://www.acer.com/ac/en/US/content/wheretobuy.

17. On information and belief, Acer Inc. has delivered the Accused eSIM Products into the stream of commerce with the expectation that they will be purchased by consumers residing in the State of Texas and in the Western District of Texas. *See* Id.

18. This Court has personal jurisdiction over Acer Inc. because, inter alia, Acer Inc., on information and belief: (1) has committed acts of patent infringement in this State and judicial district, (2) has substantial, continuous, and systematic contacts with this State and this judicial district; (3) enjoys substantial income from its operations and sales in this State and this judicial district; and (4) solicits business and markets products, systems and/or services in this State and judicial district including, without limitation, related to the Accused eSIM Products.

19. Venue is proper pursuant to 28 U.S.C. §§ 1391(c) because Acer Inc. is a foreign corporation not residing in a United States judicial district, and, therefore, they may be sued in any judicial district pursuant to 28 U.S.C. §§ 1391(c)(3).

JURISDICTION AND VENUE AS TO DEFENDANT ACER AMERICA CORPORATION

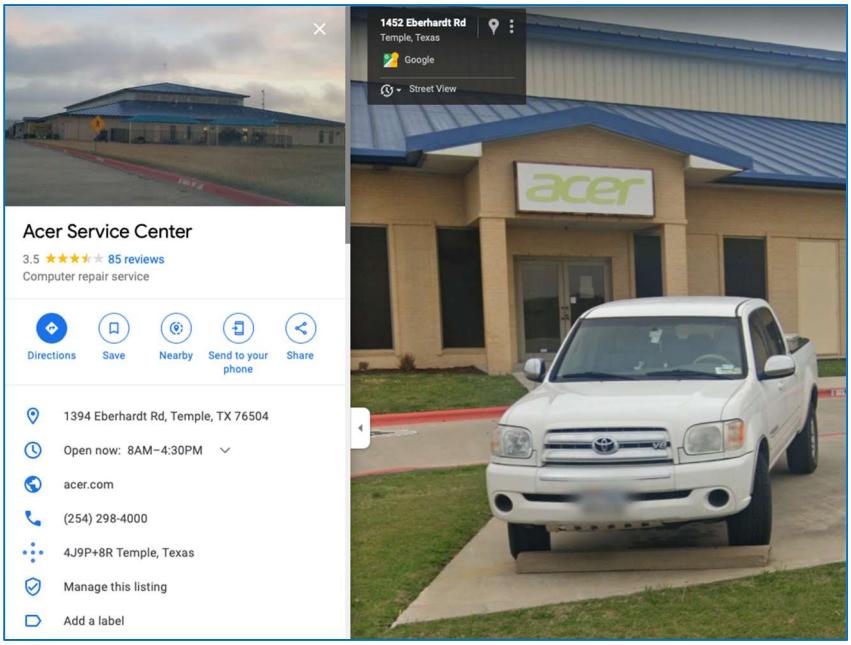
20. This Court has personal jurisdiction over Defendant Acer America Corporation because it committed and continues to commit acts of infringement in this judicial district in violation of 35 U.S.C. § 271(a). In particular, on information and belief, Acer America Corporation has made, used, offered to sell, and/or sold the Accused eSIM Products in the Western District of Texas.

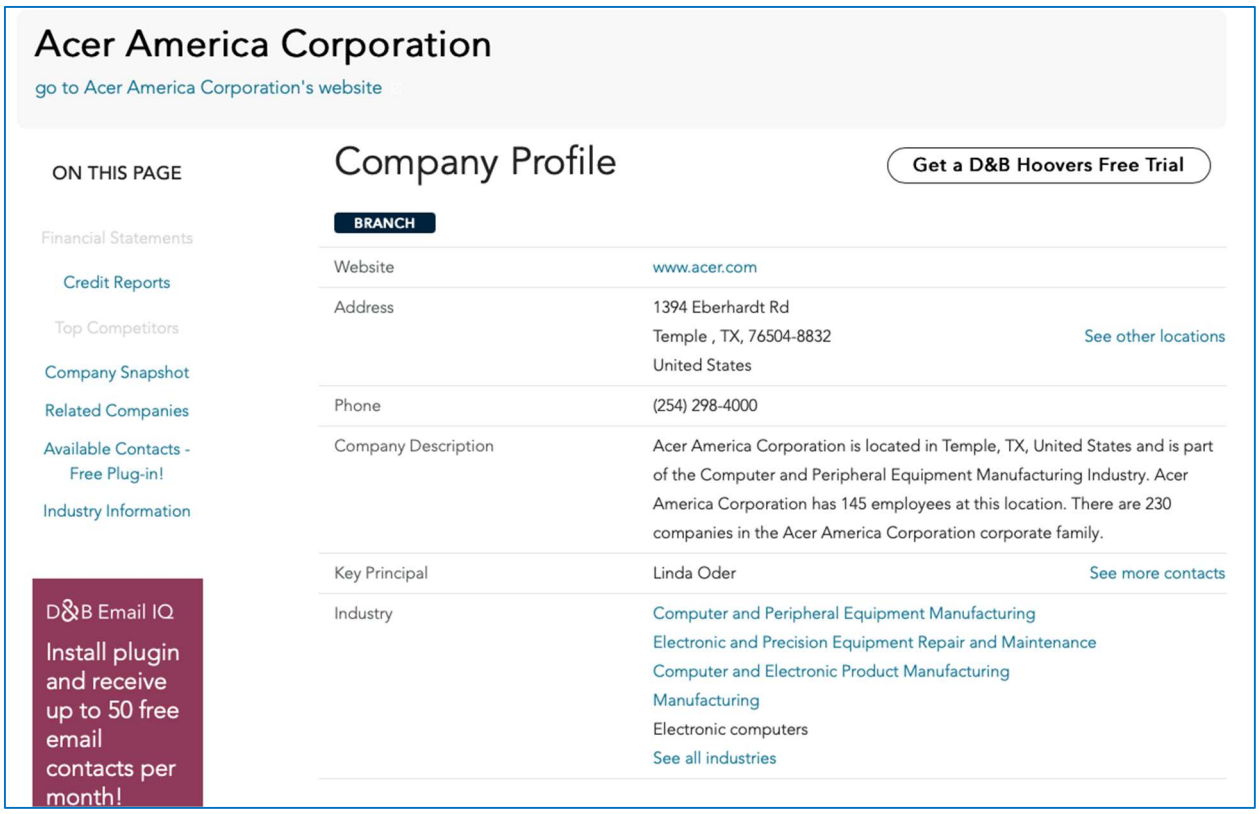
21. On information and belief, Acer America Corporation is subject to the Court's jurisdiction because it regularly conducts and solicits business, or otherwise engages in other persistent courses of conduct in this judicial district, and/or derives substantial revenue from the sale and distribution of goods and services, including but

not limited to the Accused eSIM Products provided to individuals and businesses in the Western District of Texas.

22. On information and belief, Acer America Corporation infringes the patent-in-suit in the Western District of Texas by at least making, selling, offering for sale, and/or importing, without authorization, the Accused eSIM Products.

23. On information and belief, Acer America Corporation, directly or indirectly owns and/or operates a computer repair center in the Western District of Texas located at 1394 Eberhardt Road, Temple, Texas, 96504.



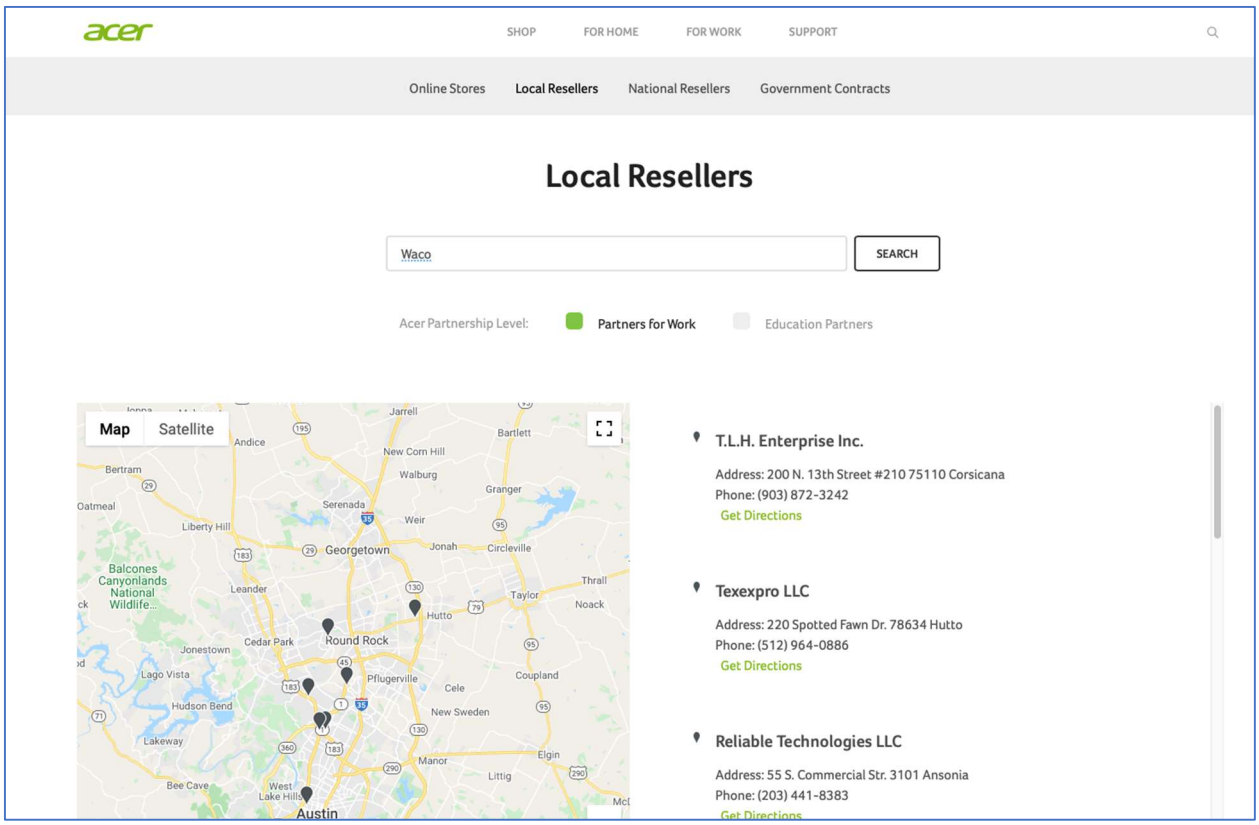


See https://www.dnb.com/business-directory/company-profiles.acer_america_corporation.5f8d9d3b820c909931a31ca1fcfb8403.html.

24. On information and belief, Acer America Corporation either directly or indirectly employs at least 145 Texas citizens in this judicial district. *See* Id.

25. On information and belief, the Accused eSIM Products are repaired and/or distributed through Acer America Corporation regular and established places of business, including its repair center located in the Western District of Texas.

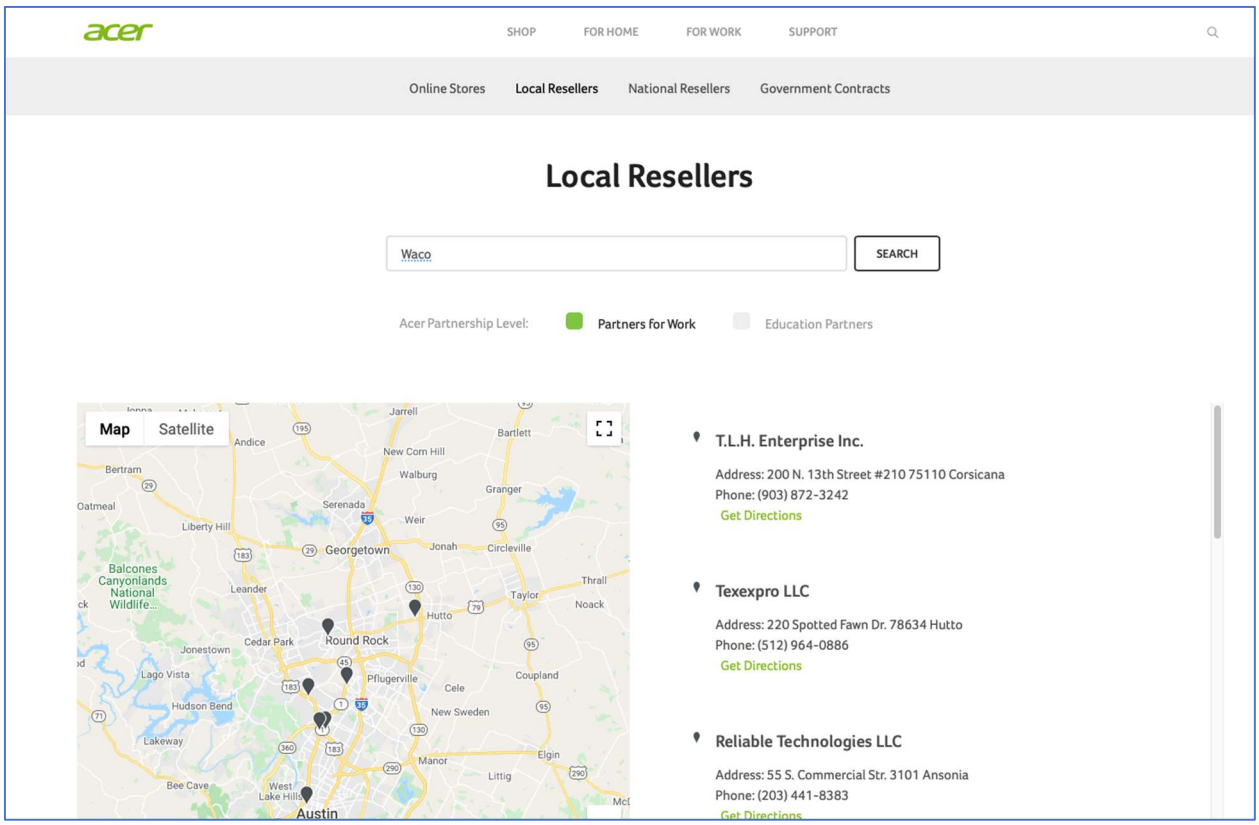
26. On information and belief, the Accused eSIM Products are sold and offered for sale in retail stores, including through Acer's "local resellers" located in the Western District of Texas.



See e.g. https://www.acer.com/ac/en/US/content/series/swift7; https://www.acer.com/ac/en/US/content/wheretobuy.

27. On information and belief, Acer America Corporation, directly and/or indirectly distributes, markets, offers to sell, and/or sells the Accused eSIM Products in the United States and/or imports the Accused eSIM Products into the United States, including in the Western District of Texas, and otherwise directs infringing activities to this Judicial District in connection with the Accused eSIM Products.

28. On information and belief, Acer America Corporation has directly or indirectly, sold and offered to sell, and the Accused eSIM Product through its website acer.com within the United States, including specifically within the Western District of Texas.



See e.g. https://www.acer.com/ac/en/US/content/series/swift7; https://www.acer.com/ac/en/US/content/wheretobuy.

29. On information and belief, Acer America Corporation has directly or indirectly imported the Accused eSIM Products into the United States, including into the Western District of Texas.

30. On information and belief, Acer America Corporation's customers located in the Western District of Texas have purchased and used the Accused eSIM Products while located in the Western District of Texas.

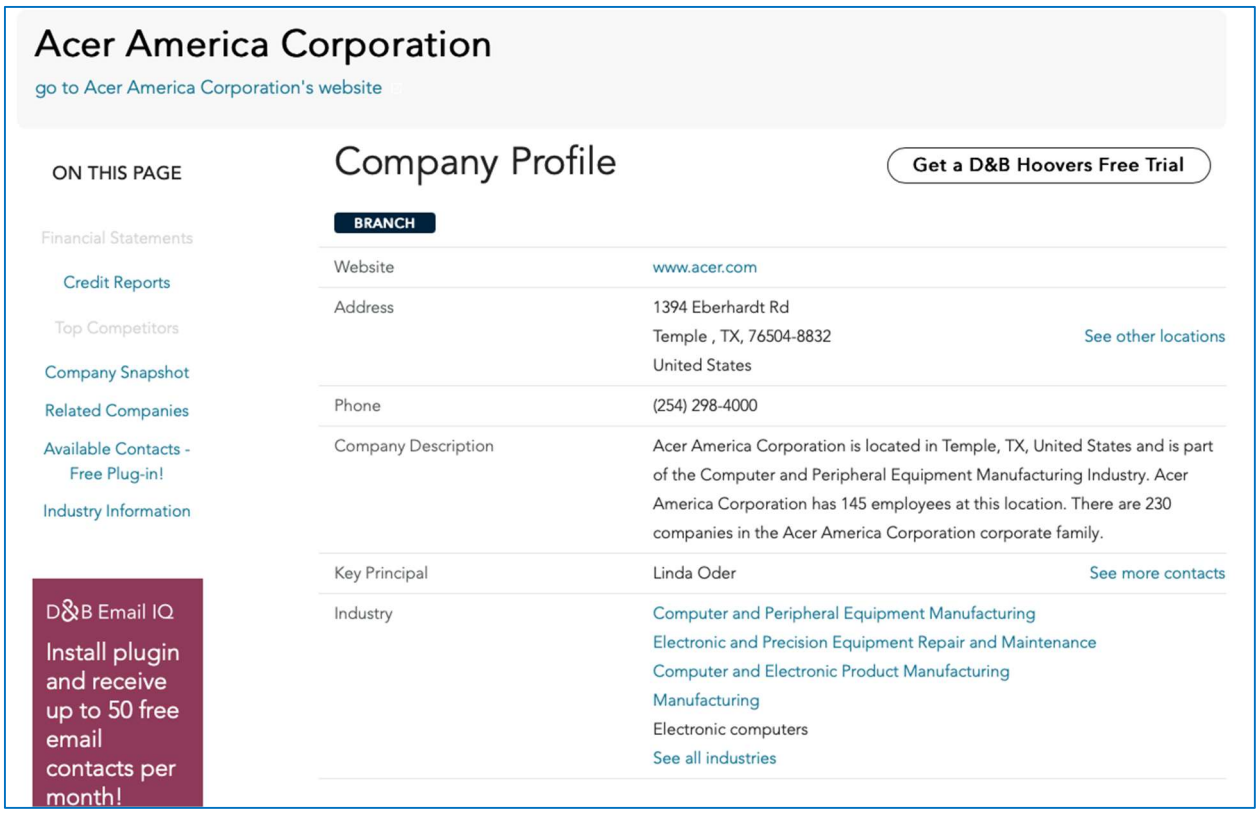
31. The Court has personal jurisdiction over Acer America Corporation at least because it has continuous business contacts in the State of Texas and in the Western District of Texas. Acer America Corporation has engaged in business activities including transacting business in the Western District of Texas and purposefully

directing its business activities, including the sale or offer for sale of the Accused eSIM Products to the Western District of Texas to aid, abet, or contribute to the infringement of third parties in the Western District of Texas.

32. This Court has personal jurisdiction over Acer America Corporation because, *inter alia*, Acer America Corporation, on information and belief: (1) has committed acts of patent infringement in this Western District of Texas; (2) maintains a regular and established place of business in the Western District of Texas; (3) has substantial, continuous, and systematic contacts with this State and the Western District of Texas; (4) owns, manages, and operates facilities in this State and the Western District of Texas; (5) enjoys substantial income from its operations and sales in this State and the Western District of Texas; (6) employs Texas residents in this State and the Western District of Texas, and (7) solicits business and markets the Accused eSIM Products in this State and the Western District of Texas.

33. Venue is proper pursuant to 28 U.S.C. §§ 1391(b), (c), (d) and/or 1400(b), at least because Acer America Corporation, has committed acts of infringement in this judicial district, and has a regular and established places of business in this judicial district.

34. On information and belief, Acer America Corporation has previously maintained and continues to maintain a regular and established places of business in this judicial district including but not limited to the regular and established place of business located at 1394 Eberhardt Road, Temple, Texas, 96504.



See https://www.dnb.com/business-directory/company-profiles.acer_america_corporation.5f8d9d3b820c909931a31ca1fcfb8403.html.

United States Patent No. 8,185,156

35. On May 22, 2012, the United States Patent and Trademark Office ("USPTO") duly and legally issued United States Patent No. 8,185,156 ("the '156 patent") entitled "Method of and Apparatus for Interfacing and Connecting a Wireless Device and a Wireless Network Using a Subscriber Identity Module Having Plural IMSI Associates With Different Network Operators" to inventors Michael Camilleri, and Jose Luis Merino Gonzalez.

36. The '156 patent is presumed valid under 35 U.S.C. § 282.

37. Shingletop owns all rights, title, and interest in the '156 patent.

38. Shingletop has not granted Acer an approval, an authorization, or a license to the rights under the '156 patent.

39. The '156 patent relates to, among other things, an improvement to the operation of the hardware, software, and operation of wireless communication devices.

40. The claimed invention(s) of the '156 patent sought to solve problems with, and improve upon, existing wireless communication technology. For example, the '156 patent states:

> Wireless devices can now handle voice and/or data, allowing simplex and/or duplex Voice calls, video calls, text messaging, and internet browsing. Some wireless communication devices can now handle voice-over-internet-protocol (VoIP) calls, and others are able to handle multimedia (voice, video, graphics) calls through wireless networks and/or through wireless networks connected to the internet or media servers.
>
> Different types of calls, initiated by wireless devices, can be restricted for some or most of their outgoing traffic; for example Voice and data calls, as well as internet web browsing, can be restricted to those call tariffs made available by the wireless network(s) that is subscribed to. Those wireless networks could be operated by traditional wireless network operators or so called virtual network operators. The restrictions can even limit which web servers the user is actually allowed to access. In most or all cases the restrictions will limit the users in their home country to only one wireless network, i.e. the home wireless network to which the user is subscribed to.
>
> Users of wireless devices subscribed to a specific wireless network in their home country, may however wish to have a choice of call set-up route(s), and also have the choice of viewing any web server or web-page that they desire, and to initiate their outgoing calls at the tariff of their choice and through any of the wireless network(s) available in their home country as well as when roaming abroad. This would give each wireless device user the freedom to choose the cheapest option for each call set-up route for any outgoing traffic. Such as outgoing-SMS, -voice call, -data call.
>
> There are several ways of achieving this, but all have drawbacks.
>
> It is known to provide a wireless device (e.g. a mobile telephone) with 2 separate SIMs, each associated with a different network operator; the 2 separate

SIMs sometimes need to be cut down to fit a single SIM reader, or else a special carrier for two SIMs is provided that itself connects to a conventional SIM package. These devices are sometimes called ghost SIMs. So, for example, a person who frequently travels between the UK and the US would have a single mobile telephone that he could use in both countries, fitted with a dual SIM ghost. If his home mobile operator is based in the UK, he would normally pay roaming charges when he makes calls from the US, call costs can be 10x greater from the US because of this. But with a dual SIM ghost on his mobile telephone, the user can toggle between SIMs by repeatedly turning the device off/on. So he can use a SIM from a US operator when in the US and a SIM from a UK operator when in the UK. But that means that incoming calls to the UK telephone number will go unanswered when the US SIM is being used, and vice versa, which is inconvenient. The user could simply toggle the phone to the US SIM only when he needs to make a call from the US, and then remember to toggle back afterwards. But that is inconvenient. And the user also has to obtain the 2 separate SIMs in the first place, which can again be inconvenient.

He could alternatively keep 2 different mobile telephones, one for use in the UK and one for the US, with each associated with a UK and US operator respectively. Then, no roaming charges will be paid when he calls from the US, because he uses the mobile telephone associated with the US operator. But having 2 different mobile telephones is costly and inconvenient, especially as people will no doubt call him on his UK mobile telephone number when he is in the US, so he would need to have both devices constantly at hand when traveling in the US.

Another solution is to have a conventional mobile telephone using just a single SIM, but to have 2 different SIMs, and to physically swap the SIM from a UK operator into the device when in the UK, and swap in a SIM from a US operator when in the US. But that is very inconvenient, and can mean that calls to the UI telephone number will just divert to voice mail when the US SIM is in use, and vice versa when the UK SIM is in use.

See '156 Specification at col. 1, l. 27 – col. 2, l. 32.

41. The '156 patent then states:

The present invention is a wireless device including a single SIM, the wireless device further including an application module adapted to enable the device to operate as though it included two or more different SIMs.

The application module may be adapted to switch the single SIM between (a) operating as a local SIM and (b) operating as a roaming SIM. The application module can be a software module that is downloaded to the device.

> The user can manually control the switching between the local SIM and roaming SIM operation; switching can for example be done by an end-user operating a Switch, or an end-user interacting with an on-screen menu displayed on the device.

See '156 Specification at col. 3, ll. 7-19.

42. The '156 patent then states:

> The local SIM sub-module and the roaming SIM sub-module are sub-modules within the single SIM (so that, for example, the application module, although in the wireless device, is not part of the SIM itself). Alternatively, the application module, the local SIM sub-module and the roaming SIM sub-module are each sub-modules within the single SIM.

See '156 Specification at col. 3, ll. 47-53.

43. The '156 patent then states:

> The present invention can enable communications with a mobile virtual network operator, virtual telecoms operator or a virtual telecoms provider. The wireless device itself can be a mobile telephone, wireless card, Smart phone or wireless module.

See '156 Specification at col. 4, ll. 7-11.

44. The '156 patent then states in reference to Figure 2:

> The WD1 with a built-in PAM 2 establishes data communication between the WD 1 and a wireless network 4-5 coupled to a digital communication system associated with one of the Local SIM (LS) 21 or Roaming SIM (RS) 22 identities; both LS 21 and RS 22 are embedded into a single SIM, and are each defined by a unique IMSI number. As a first step, the PAM 2. 2n chooses either the Local SIM (LS) 21 or Roaming SIM (RS) 22 identity. The WD1 provides location updates each time the PAM 2 (e.g. built into the WD) changes SIM identity (e.g. selects a different SIM sub-module, LS 21 or RS 22, each embedded into the single SIM, which itself resides in the WD 1. Each sub-module LS 21 and RS 22 is associated with a different IMSI and therefore network operator. WD 1 also provides a location update each time it changes wireless network name or wireless network country or region or state.

See '156 Specification at col. 6, ll. 10-25.

45. The invention(s) claimed in the '156 patent solves various technological problems inherent in the then-existing wireless communication systems and devices, and enables such systems and devices to, among other things: (1) function more efficiently; (2) operate as though the device included two or more different SIMs; and (3) simplify the manner in which a user operates said systems and devices to achieve the claimed functionality.

United States Patent No. 8,467,831

46. On June 18, 2013, the USPTO duly and legally issued United States Patent No. 8,467,831 ("the '831 patent") entitled "Method of and Apparatus for Interfacing and Connecting a Wireless Device and a Wireless Network Using a Subscriber Identity Module Having Plural IMSI Associates With Different Network Operators" to inventors Michael Camilleri, and Jose Luis Merino Gonzalez.

47. The '831 patent is presumed valid under 35 U.S.C. § 282.

48. Shingletop owns all rights, title, and interest in the '831 patent.

49. Shingletop has not granted Acer an approval, an authorization or a license to the rights under the '831 patent.

50. The '831 patent relates to, among other things, an improvement to the operation of the hardware, software, and operation of wireless communication devices.

51. The specification of the '831 patent is the same as the '156 patent specification, and solves the problems recited above and described in the '156 patent specification.

United States Patent No. 9,532,208

52. On December 27, 2016, the USPTO duly and legally issued United States Patent No. 9,532,208 ("the '208 patent") entitled "Method of and Apparatus for Interfacing and Connecting a Wireless Device and a Wireless Network Using a Subscriber Identity Module Having Plural IMSI Associates With Different Network Operators" to inventors Michael Camilleri, and Jose Luis Merino Gonzalez.

53. The '208 patent is presumed valid under 35 U.S.C. § 282.

54. Shingletop owns all rights, title, and interest in the '208 patent.

55. Shingletop has not granted Acer an approval, an authorization or a license to the rights under the '208 patent.

56. The '208 patent relates to, among other things, an improvement to the operation of the hardware, software, and operation of wireless communication devices.

57. The specification of the '208 patent is the same as the '156 patent and '831 patent specifications, and solves the problems recited above and described in the '156 patent and '831 patent specifications.

CLAIMS FOR RELIEF

Count I – Infringement of United States Patent No. 8,185,156

58. Shingletop repeats, realleges, and incorporates by reference, as if fully set forth here, the allegations of the preceding paragraphs above.

59. On information and belief, Acer (or those acting on its behalf) makes, uses, sells access to, and/or offers to sell access to the Accused eSIM Products that infringe

(literally and/or under the doctrine of equivalents) at least claims 1, 18, 19, and 20 of the '156 patent.

60. On information and belief, the Accused eSIM Products conform to the requirements of the GSMA Remote SIM Provisioning standards,[12] which include SGP.02[13] and SGP.22.[14] On information and belief, the GSMA Remote SIM Provisioning standards are described by "eSIM Whitepaper: The what and how of Remote SIM Provisioning"[15] and "GSMA Embedded SIM Specification Remote SIM Provisioning for M2M."[16]

61. On information and belief, the Accused eSIM Products employ and provide a method of communicating with a wireless network, as demonstrated by the standards, images, diagrams, tables, and documents cited below.

[12] *See* https://www.businesswire.com/news/home/20180530005103/en/Want-to-Have-4G-Connectivity-on-your-PC-Everywhere-you-go-With-Acer-and-Gemalto-you-can.

[13] *See* https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf.

[14] *See* https://www.gsma.com/newsroom/wp-content/uploads/SGP.22_v2.2.pdf.

[15] *See* https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf.

[16] *See* https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf.

GSM Association Non-confidential
Official Document SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification

GSMA

Remote Provisioning Architecture for Embedded UICC Technical Specification

Version 3.2

27 June 2017

See https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf at p. 1.

GSM Association Non-confidential
Official Document SGP.22 - RSP Technical Specification

GSMA

RSP Technical Specification

Version 2.2

01 September 2017

See https://www.gsma.com/newsroom/wp-content/uploads/SGP.22_v2.2.pdf at p. 1.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

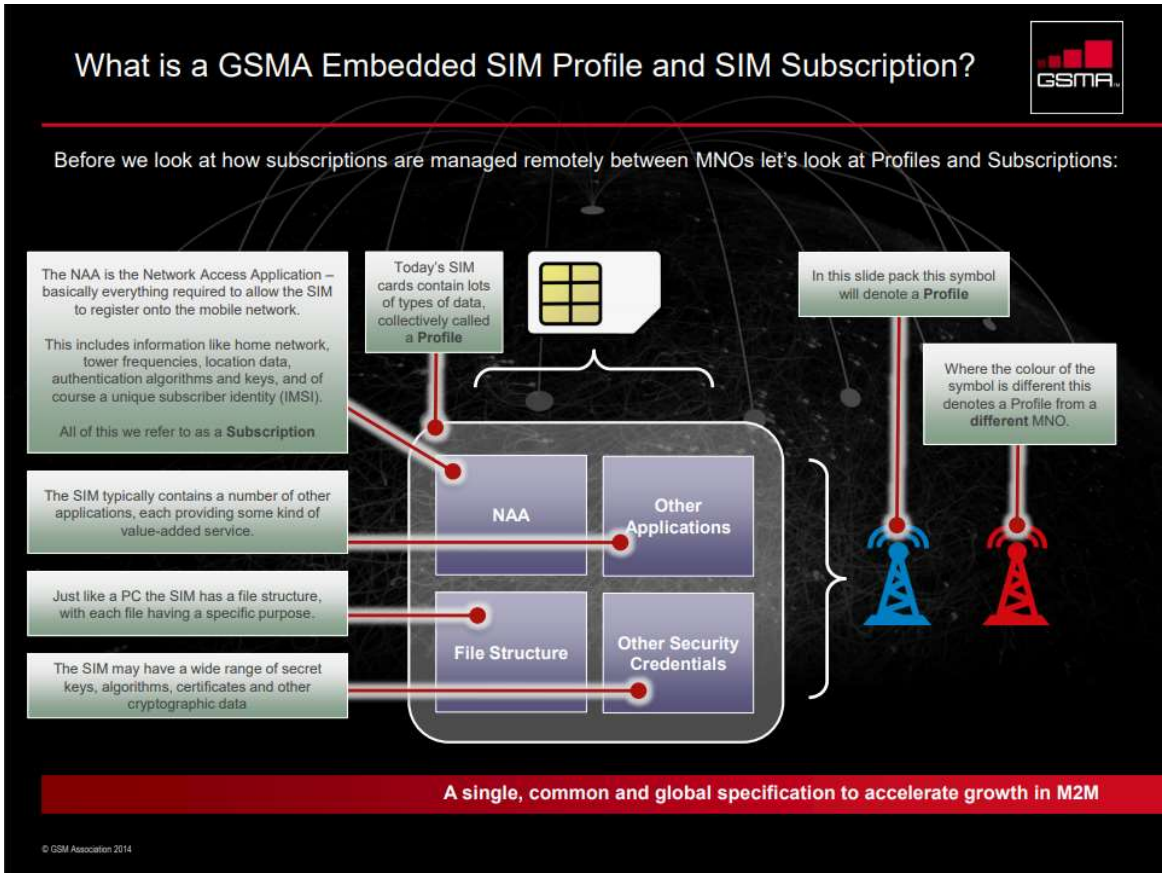
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

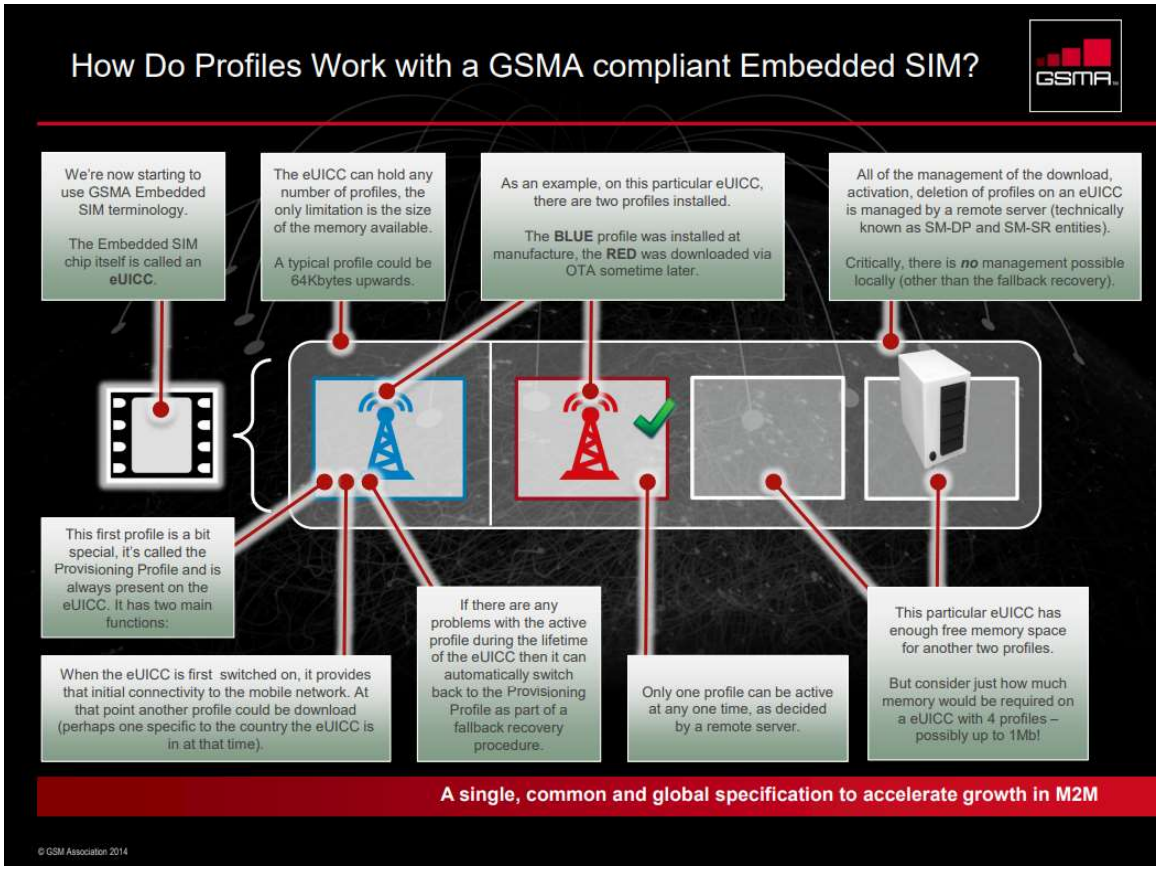
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

62. On information and belief, the Accused eSIM Products employ and provide a method comprising the step using a wireless device including a single SIM, the wireless device further including an application module adapted to enable the device to operate as though it included two or more different SIMs in which the device includes two SIM sub-modules, each with a different IMSI, as demonstrated by the standards, images, diagrams, and document cited below.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

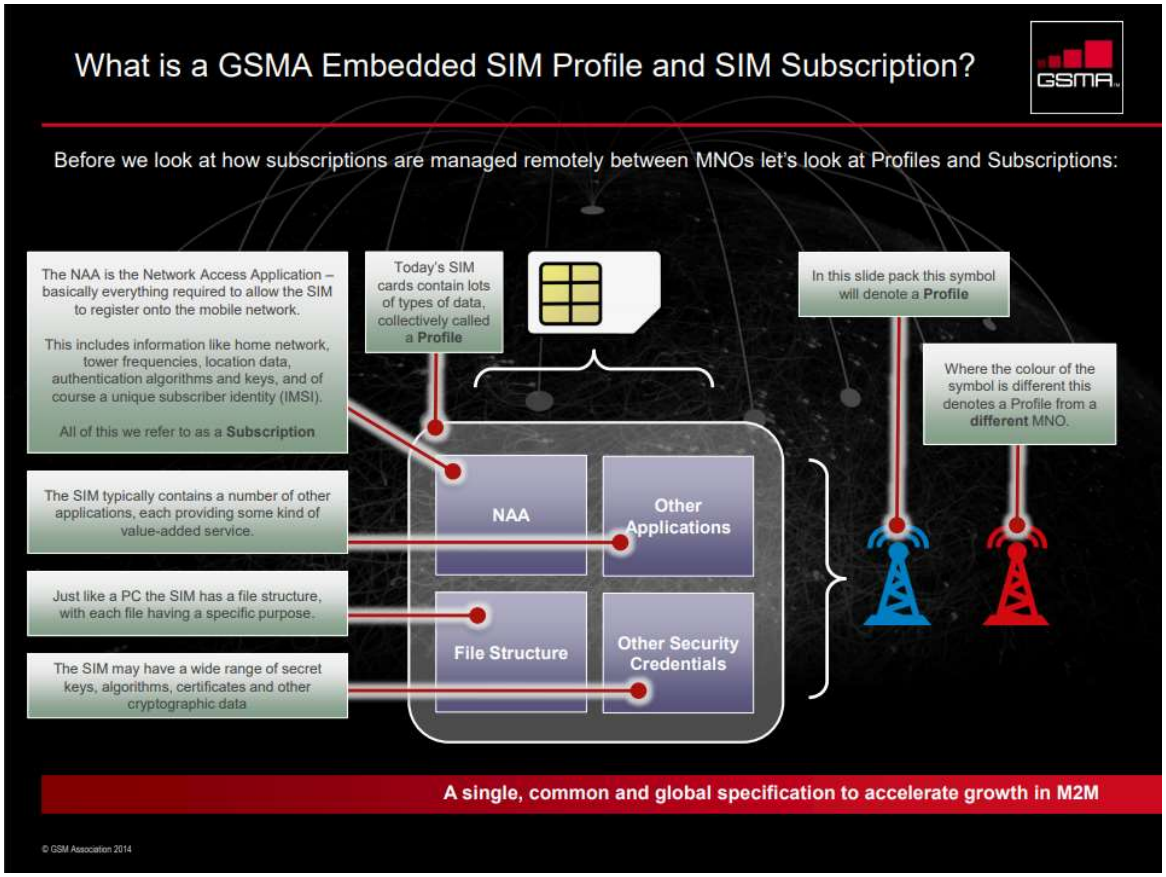
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

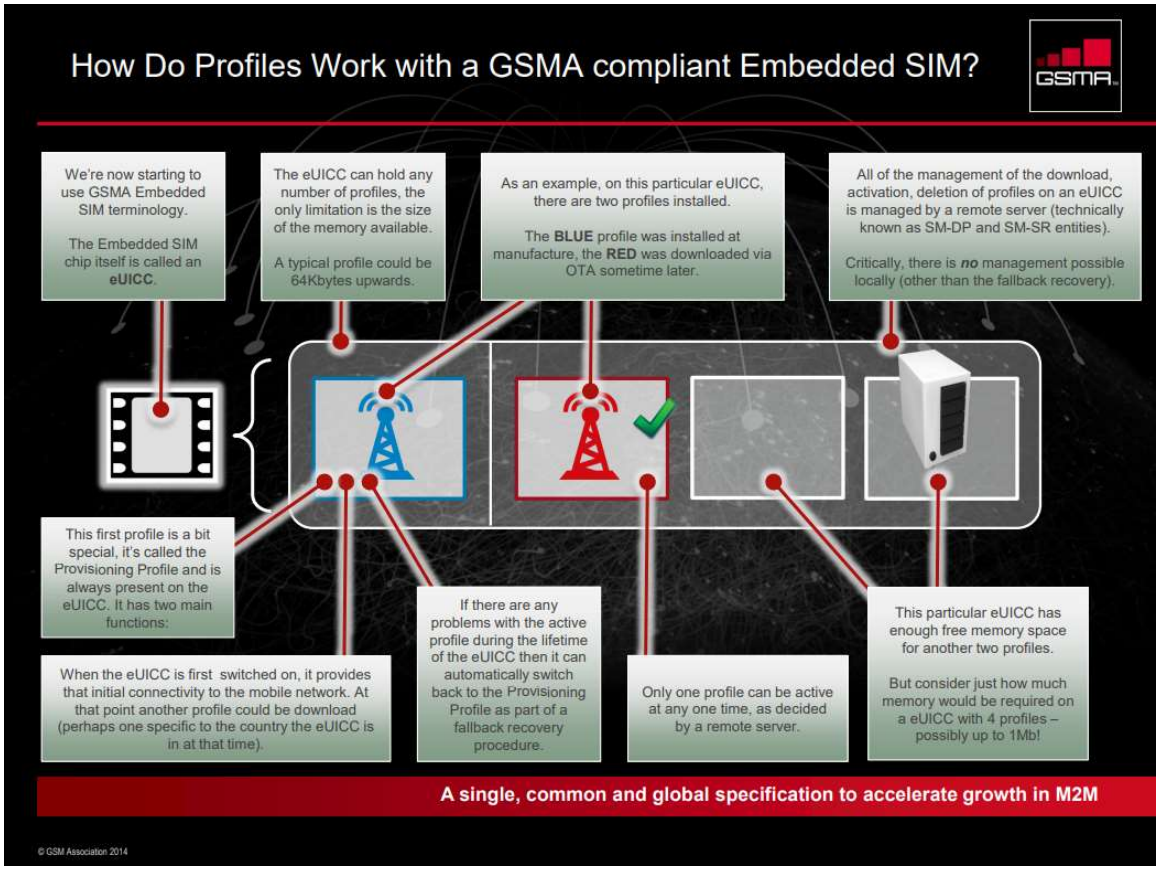
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

63. On information and belief, the Accused eSIM Products employ and provide a method comprising the step using the wireless device further including an application module adapted to switch the single SIM between (a) operating as a local SIM using the first sub-module, which is associated with a network operating 1 based in country A and (b) operating as a roaming SIM using the second sub-module, which is associated with a network operator 2 based in country B, the switching occurring inside country A under manual control of a user to obtain lower cost routing when in that country A, as demonstrated by the standards, images, diagrams, and document cited below.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

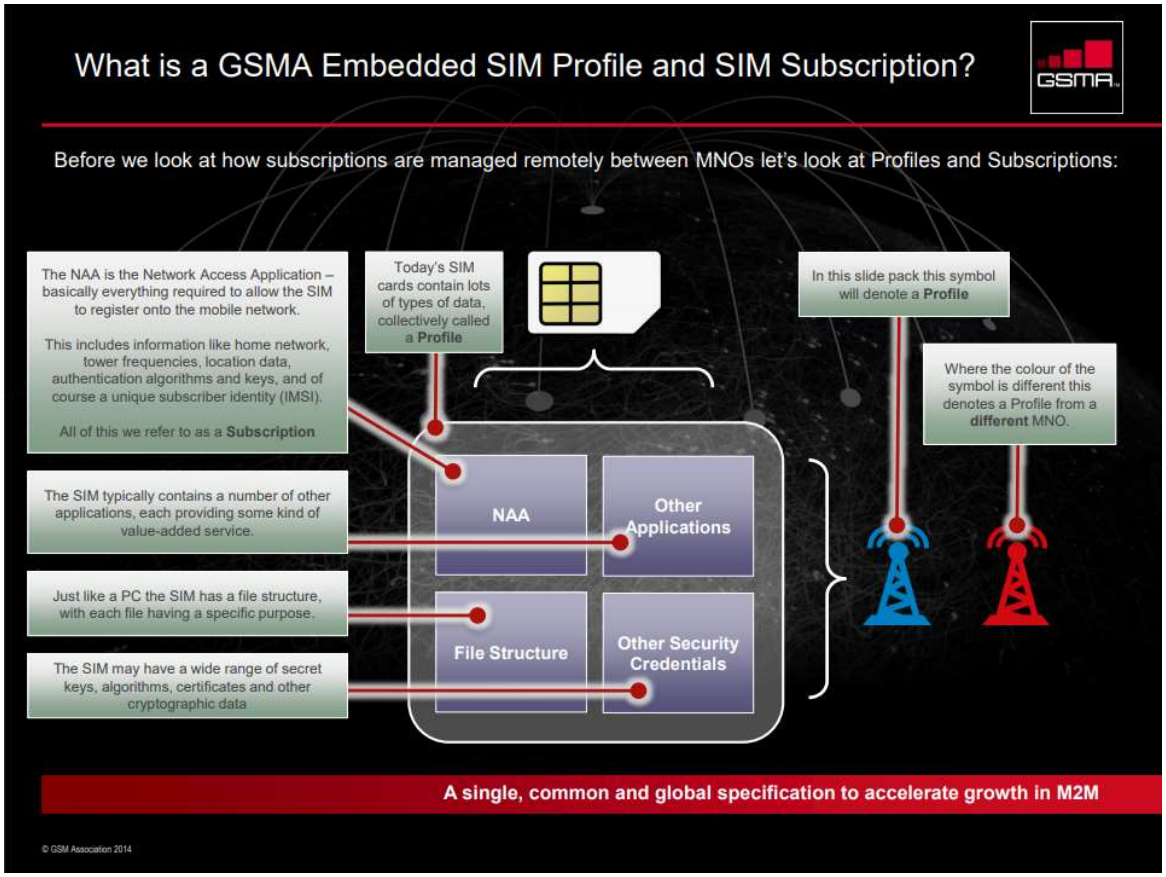
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

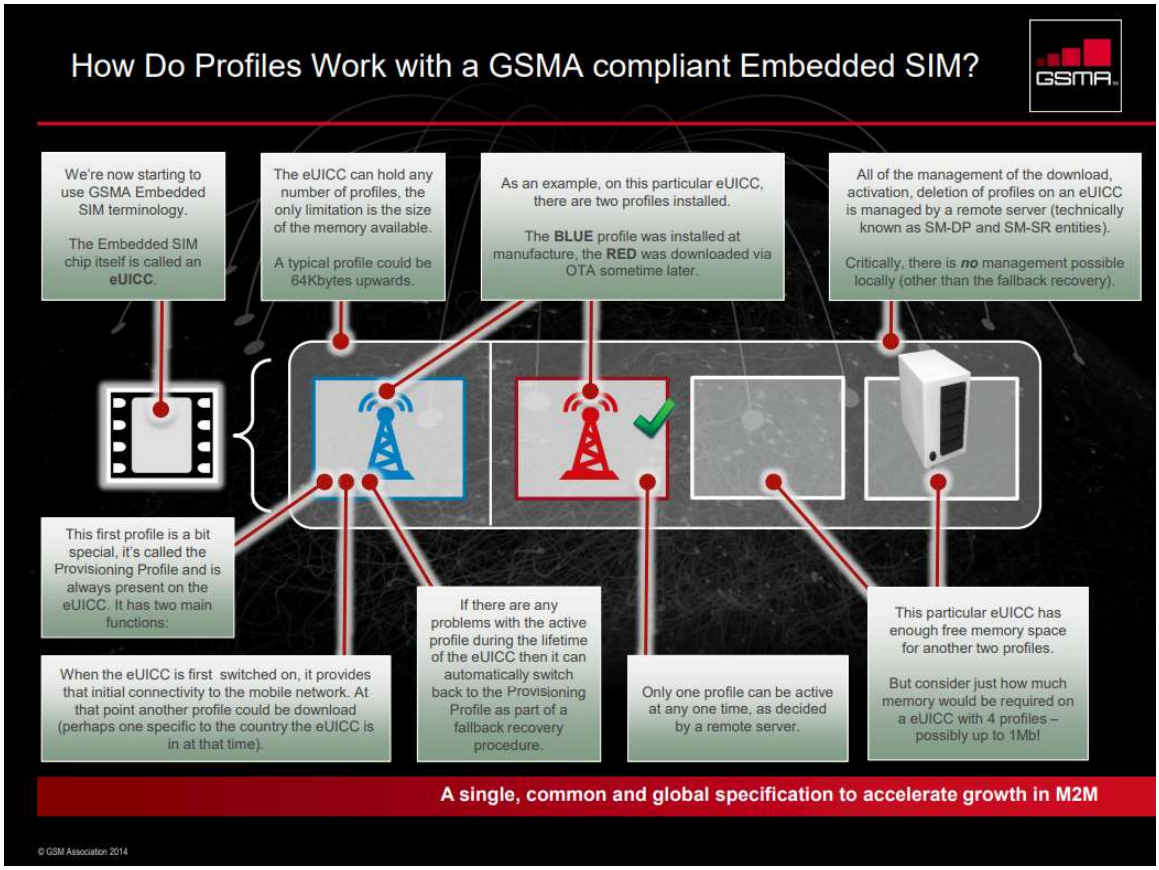
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

64. On information and belief, Acer directly infringes at least claims 1, 18, 19, and 20 of the '156 patent, and is in violation of 35 U.S.C. § 271(a) by making, using, selling, and offering to sell the Accused eSIM Products.

65. Acer's direct infringement has damaged Shingletop and caused it to suffer and continue to suffer irreparable harm and damages.

Count II – Infringement of United States Patent No. 8,467,831

66. Shingletop repeats, realleges, and incorporates by reference, as if fully set forth here, the allegations of the preceding paragraphs above.

67. On information and belief, Acer (or those acting on its behalf) makes, uses, sells access to, and/or offers to sell access to the Accused eSIM Products that infringe (literally and/or under the doctrine of equivalents) at least claims 1, 18, 19, and 20 of the '831 patent.

68. On information and belief, the Accused eSIM Products conform to the requirements of the GSMA Remote SIM Provisioning standards,[17] which include SGP.02[18] and SGP.22.[19] On information and belief, the GSMA Remote SIM Provisioning standards are described by "eSIM Whitepaper: The what and how of Remote SIM Provisioning"[20] and "GSMA Embedded SIM Specification Remote SIM Provisioning for M2M."[21]

69. On information and belief, the Accused eSIM Products employ and provide a method of communicating with a wireless network, as demonstrated by the standards, images, diagrams, tables, and documents cited below.

[17] *See* https://www.businesswire.com/news/home/20180530005103/en/Want-to-Have-4G-Connectivity-on-your-PC-Everywhere-you-go-With-Acer-and-Gemalto-you-can.

[18] *See* https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf.

[19] *See* https://www.gsma.com/newsroom/wp-content/uploads/SGP.22_v2.2.pdf.

[20] *See* https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf.

[21] *See* https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf.

GSM Association Non-confidential
Official Document SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification

GSMA

Remote Provisioning Architecture for Embedded UICC Technical Specification

Version 3.2

27 June 2017

See https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf at p. 1.

GSM Association Non-confidential
Official Document SGP.22 - RSP Technical Specification

GSMA

RSP Technical Specification

Version 2.2

01 September 2017

See https://www.gsma.com/newsroom/wp-content/uploads/SGP.22_v2.2.pdf at p. 1.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

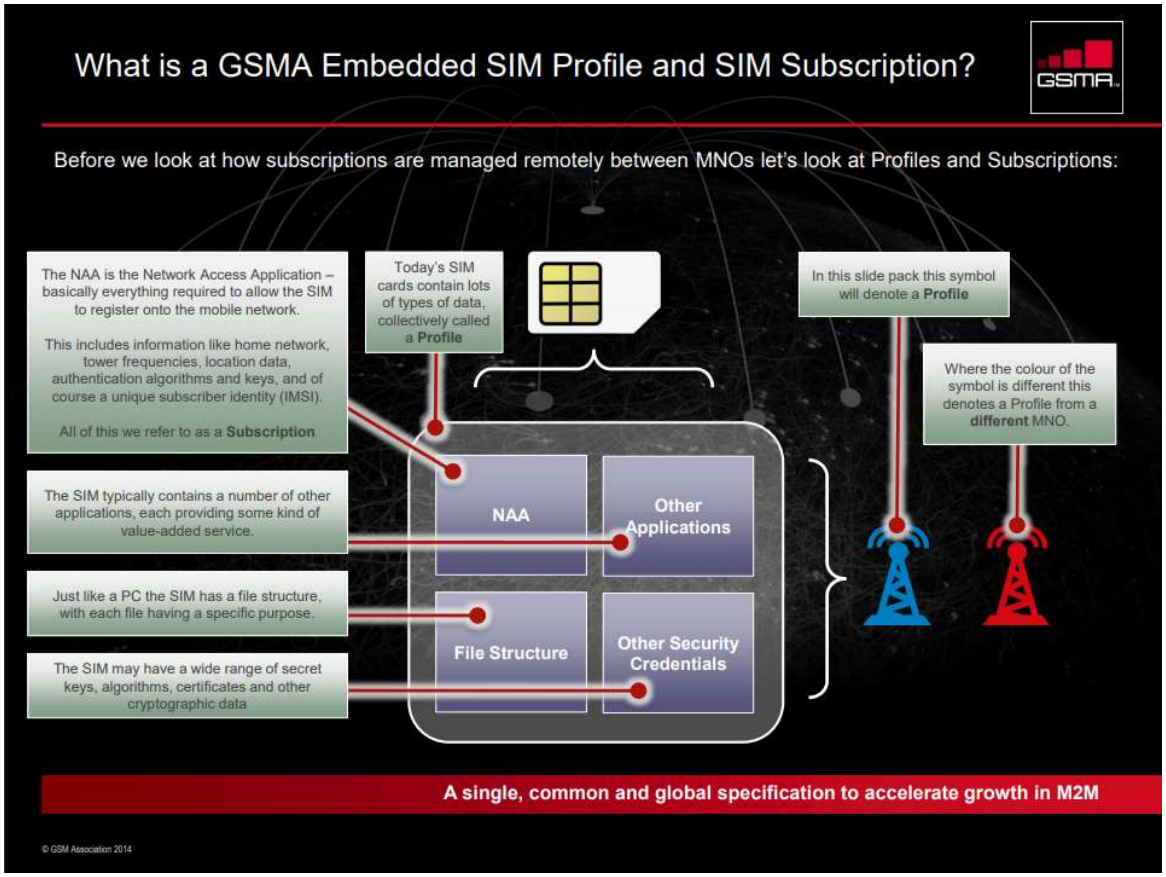
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

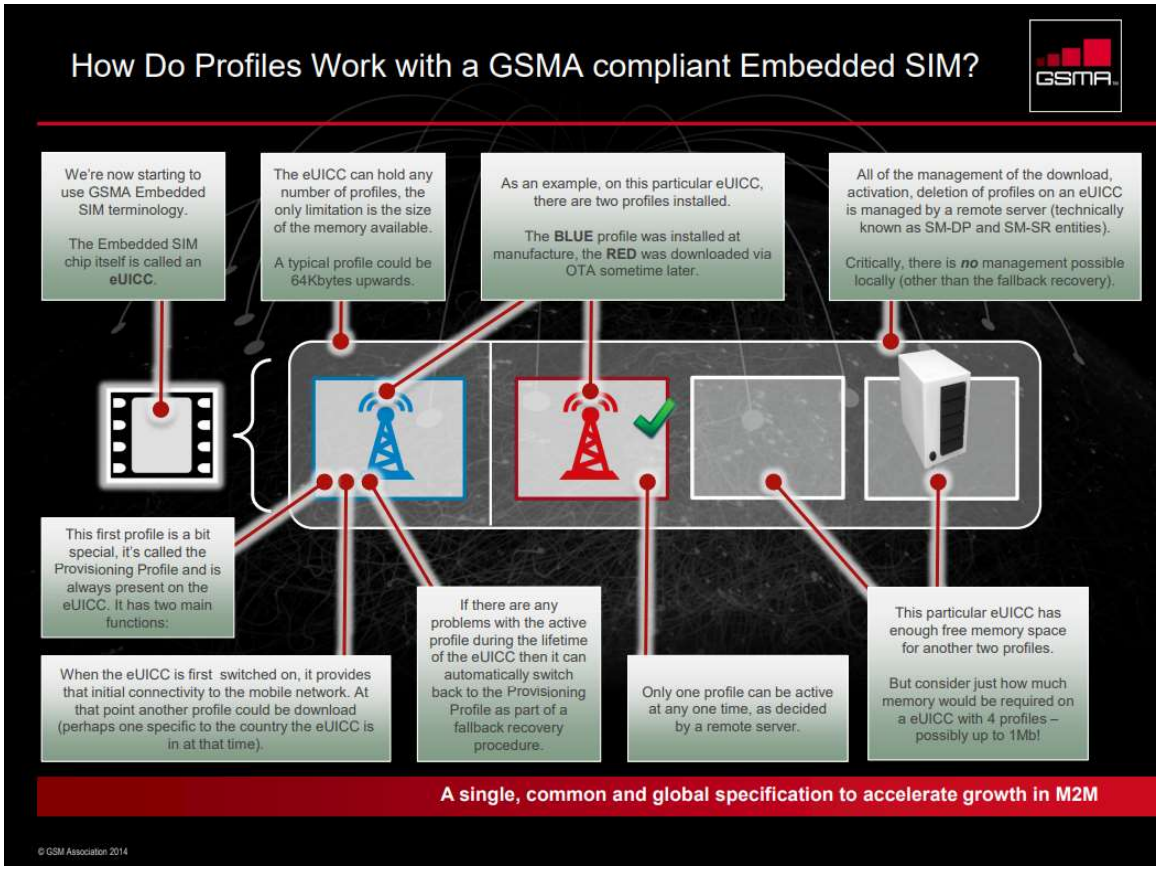
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

70. On information and belief, the Accused eSIM Products employ and provide a method comprising the step using a wireless device including a single SIM, the wireless device further including an application module adapted to enable the device to operate as though it included two or more different SIMs in which the device includes two SIM sub-modules, each with a different IMSI, as demonstrated by the standards, images, diagrams, and document cited below.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

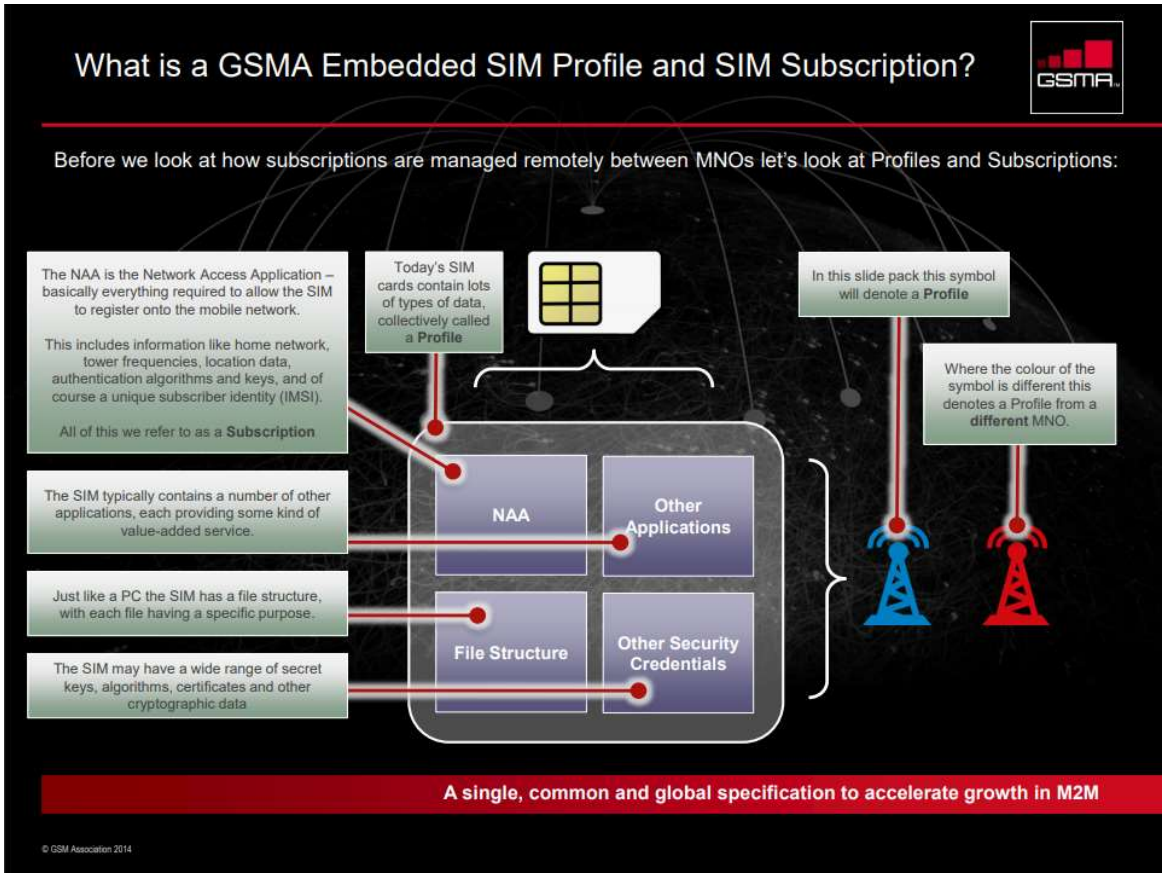
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

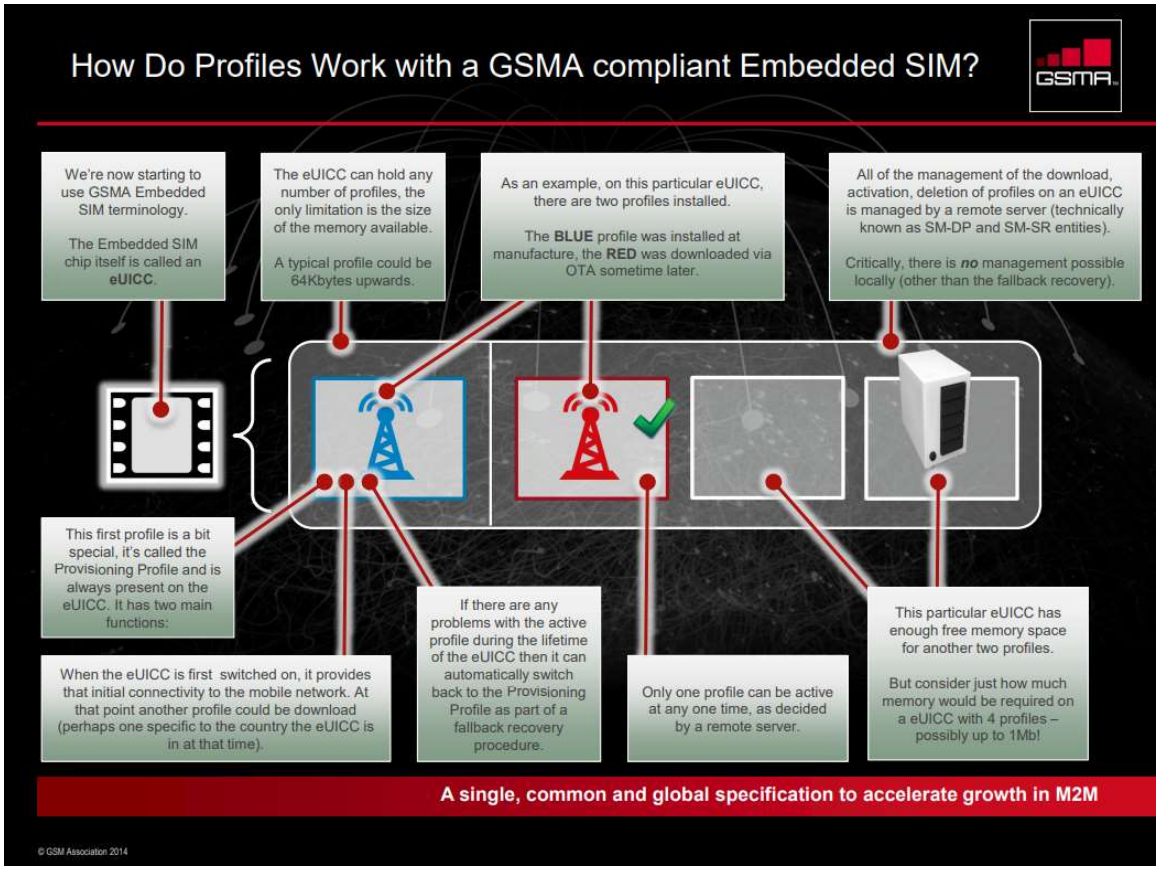
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

71. On information and belief, the Accused eSIM Products employ and provide a method comprising the step using the wireless device further including an application module adapted to switch the single SIM between (a) operating as a local SIM using the first sub-module, which is associated with a network operating 1 based in country A and (b) operating as a roaming SIM using the second sub-module, which is associated with a network operator 2 based in country B, the switching occurring inside country A under manual control of a user to obtain lower cost routing when in that country A and in which, at power-on, the sub-module operating as a local SIM is selected by default, as demonstrated by the standards, images, diagrams, and document

cited below.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

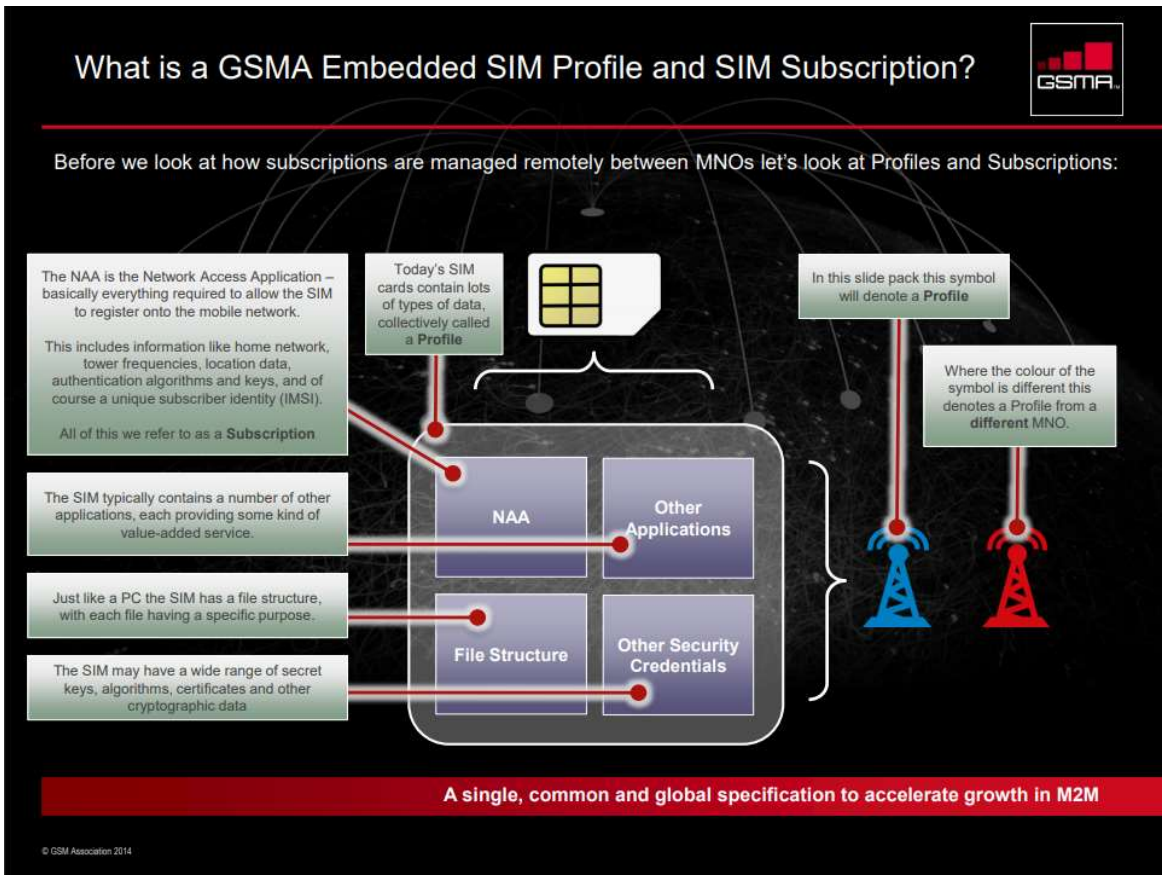
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

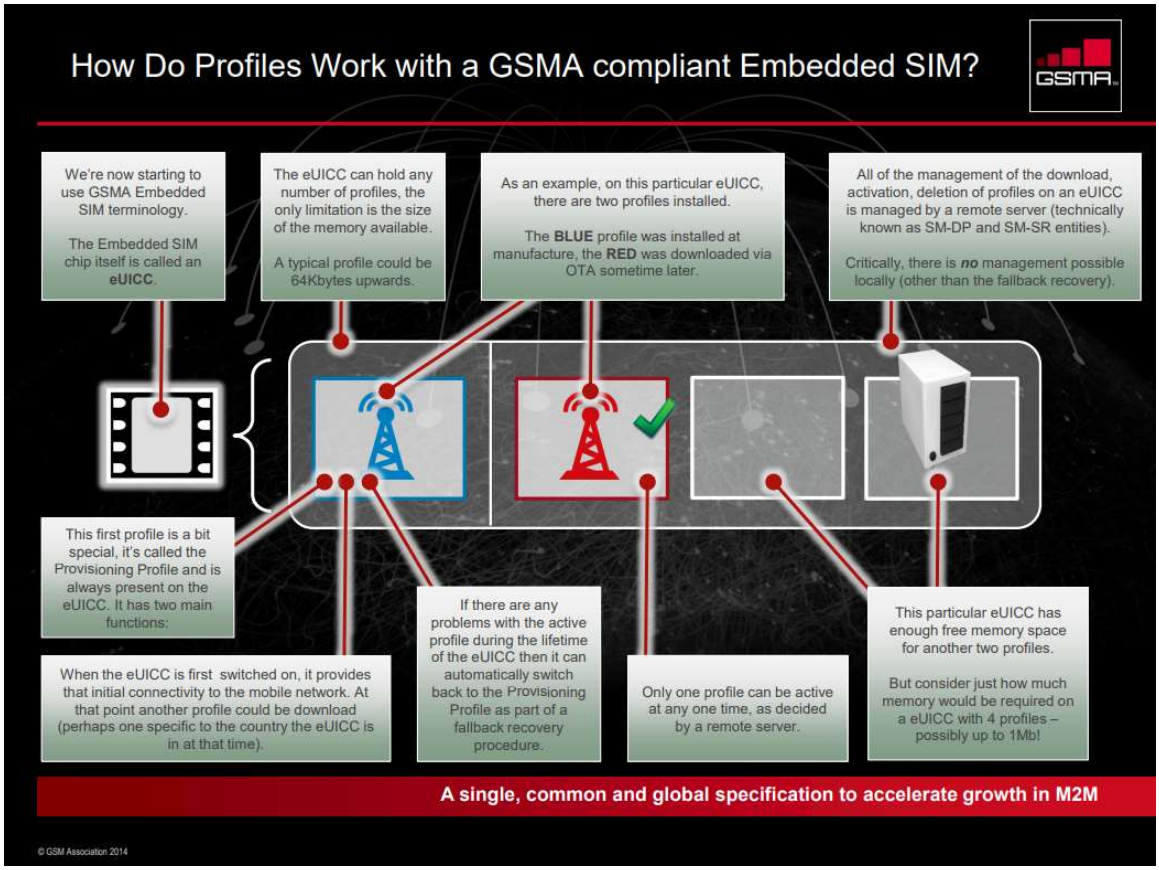
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

72. On information and belief, Acer directly infringes at least claims 1, 18, 19, and 20 of the '831 patent, and is in violation of 35 U.S.C. § 271(a) by making, using, selling, and offering to sell the Accused eSIM Products.

73. Acer's direct infringement has damaged Shingletop and caused it to suffer and continue to suffer irreparable harm and damages.

Count III – Infringement of United States Patent No. 9,532,208

74. Shingletop repeats, realleges, and incorporates by reference, as if fully set forth here, the allegations of the preceding paragraphs above.

75. On information and belief, Acer (or those acting on its behalf) makes, uses, sells access to, and/or offers to sell access to the Accused eSIM Products that infringe (literally and/or under the doctrine of equivalents) at least claims 1, 8, and 13 of the '208 patent.

76. On information and belief, the Accused eSIM Products conform to the requirements of the GSMA Remote SIM Provisioning standards,[22] which include SGP.02[23] and SGP.22.[24] On information and belief, the GSMA Remote SIM Provisioning standards are described by "eSIM Whitepaper: The what and how of Remote SIM Provisioning"[25] and "GSMA Embedded SIM Specification Remote SIM Provisioning for M2M."[26]

77. On information and belief, the Accused eSIM Products employ and provide a system including: (i) a wireless device including a single SIM, the SIM further including a downloadable first software application module embodied on a non-transitory storage medium, the first Software application module controlling switching between sub-modules in the single SIM, namely a local SIM sub-module part of the first software application module with a first International Mobile Subscriber

---

[22] *See* https://www.businesswire.com/news/home/20180530005103/en/Want-to-Have-4G-Connectivity-on-your-PC-Everywhere-you-go-With-Acer-and-Gemalto-you-can.

[23] *See* https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf.

[24] *See* https://www.gsma.com/newsroom/wp-content/uploads/SGP.22_v2.2.pdf.

[25] *See* https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf.

[26] *See* https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf.

Identity (IMSI) associated with a network operator based in country A, and a second SIM sub-module part of the first software application module with a different IMSI which is associated with a network operator based in country B, as demonstrated by the standards, images, diagrams, tables, and documents cited below.

See https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf at p. 1.

See https://www.gsma.com/newsroom/wp-content/uploads/SGP.22_v2.2.pdf at p. 1.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

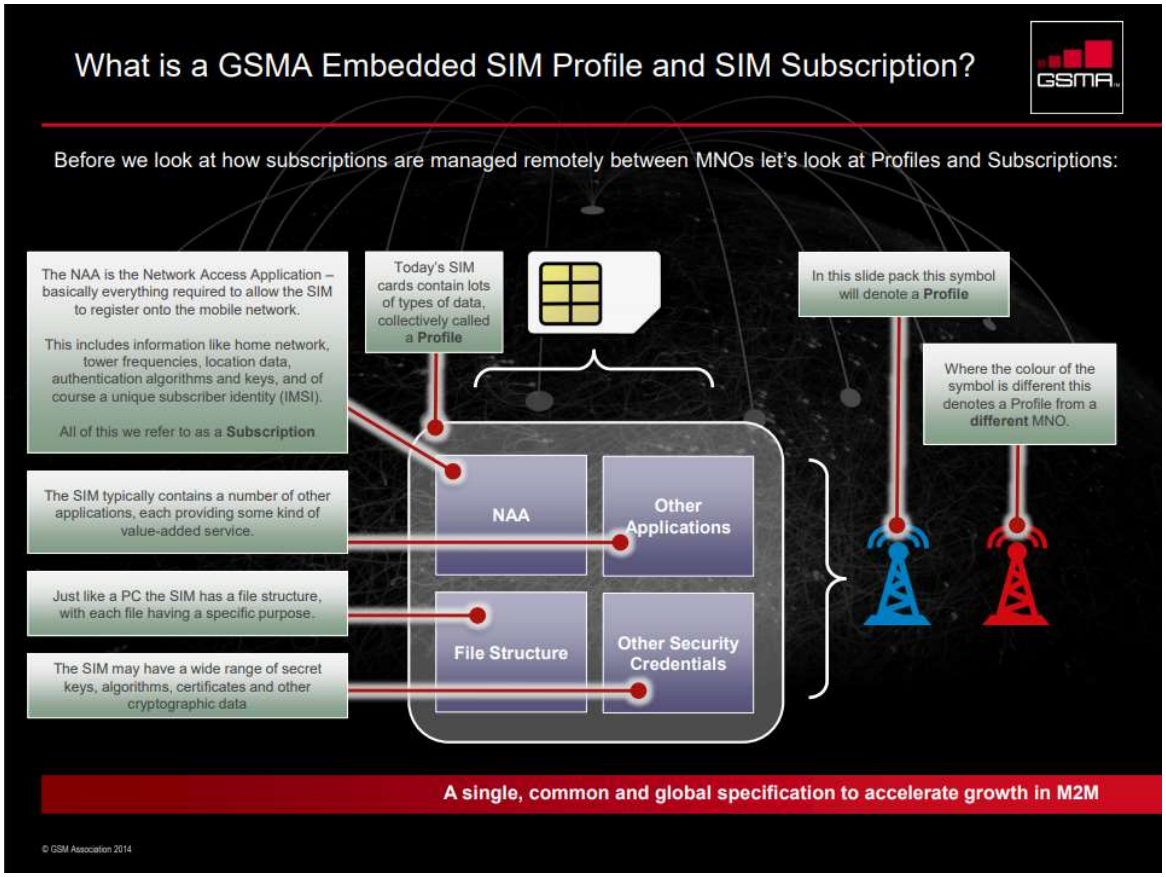
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

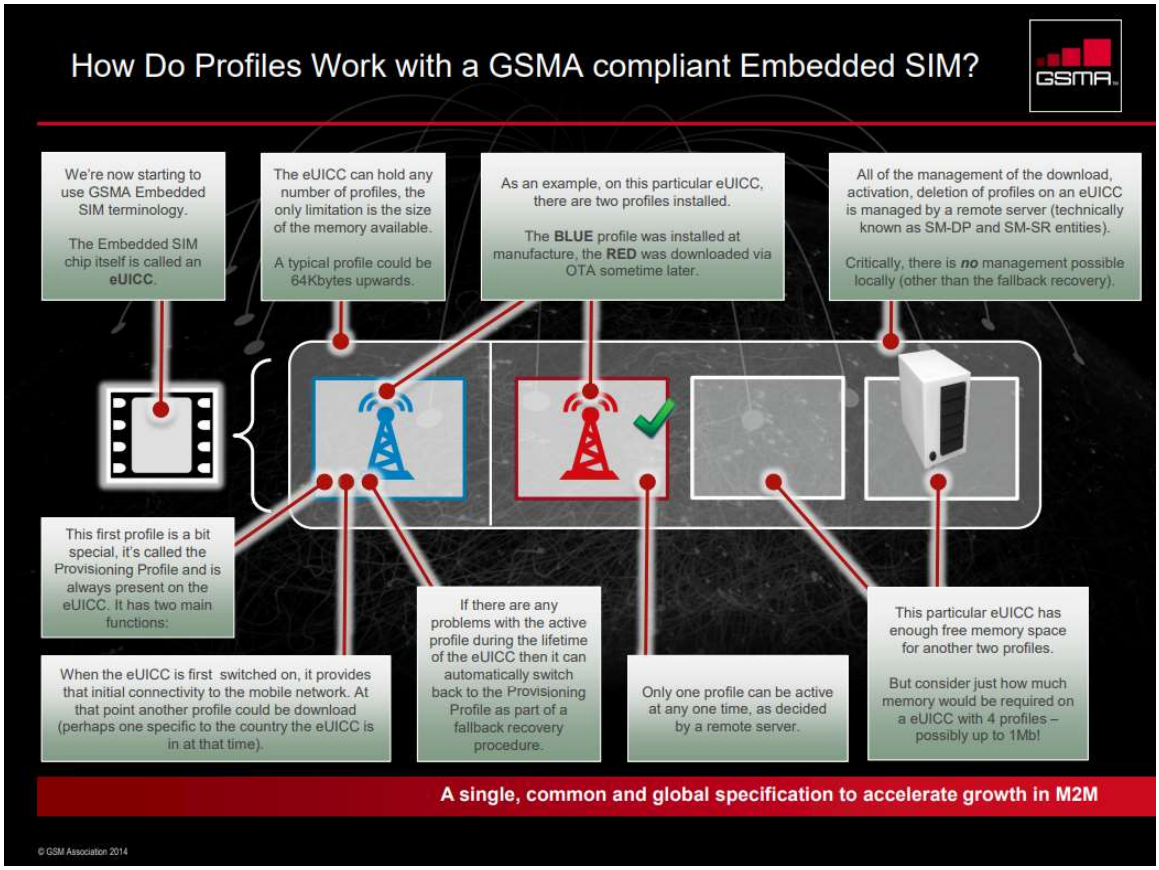
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

78. On information and belief, the Accused eSIM Products employ and provide a system including: (ii) an external switch sub-module part of a second software application module embodied on a non-transitory storage medium that is adapted to communicate with the wireless device, as demonstrated by the standards, images, diagrams, and document cited below.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

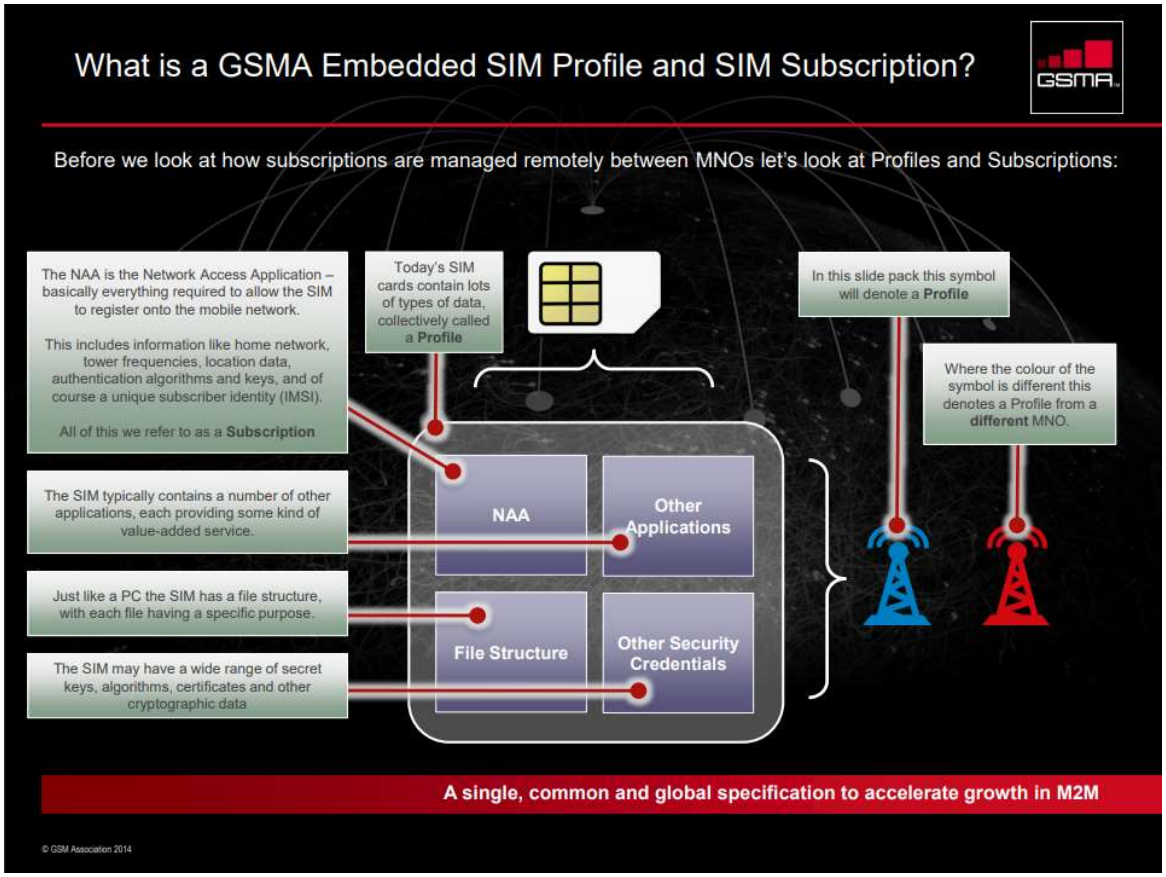
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

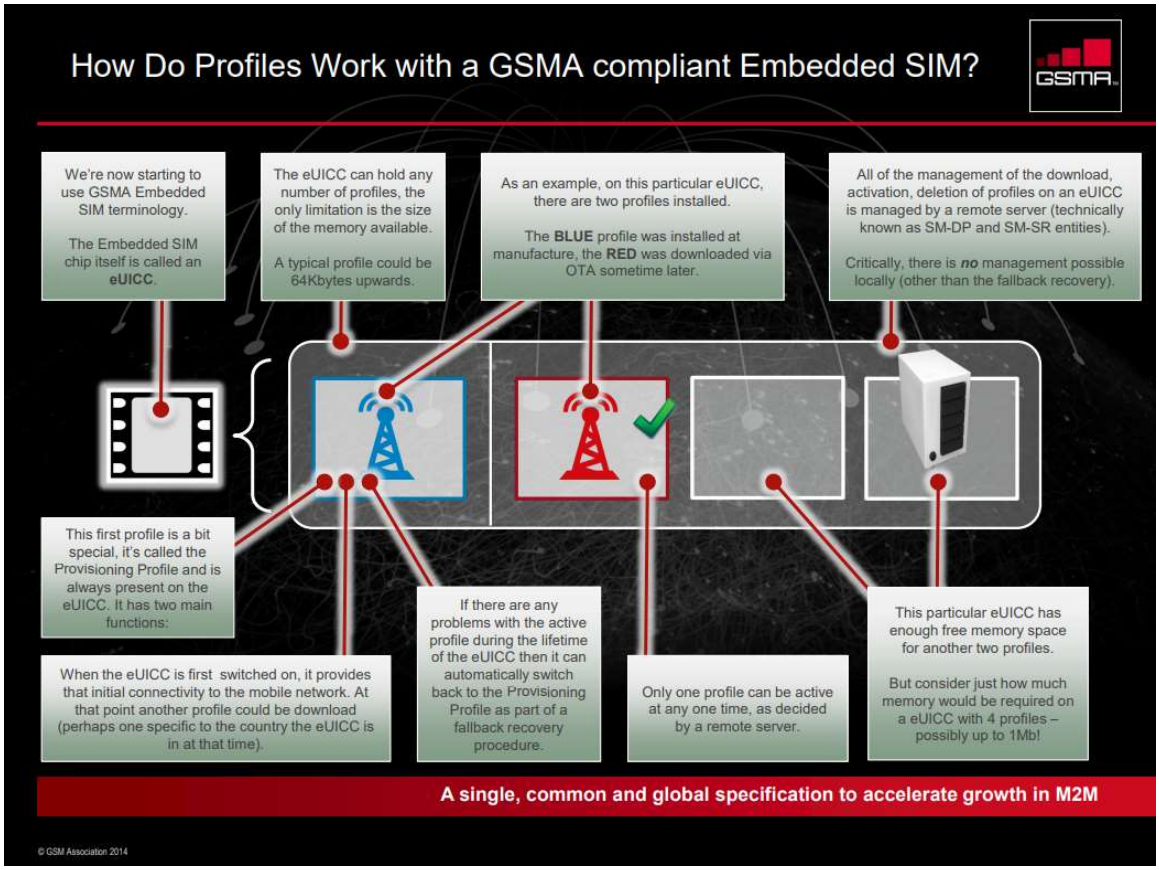
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

79. On information and belief, the Accused eSIM Products employ and provide a system including: wherein the external switch sub-module part of the second software application module controls the switching by the first software application module between the sub-modules of the single SIM, as demonstrated by the standards, images, diagrams, and document cited below.

Remote SIM Provisioning

With Remote SIM Provisioning, there are no traditional SIM cards[1]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card (the red and blue dots in the previous section). An example is illustrated in the following figure.

Remote SIM Provisioning Operation – Operator Profile Installation

In (1), the end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. In this example a QR (Quick Response) code is used. The QR code contains the address of the Remote SIM Provisioning system (SM-DP+ server within the GSMA specifications), which allows the device to connect to that system (2) and securely download a SIM Profile. Once the Profile is installed and activated, the device is able to connect to that operator's network (3).

It should be noted that the use of QR codes is one way that the eSIM solution can be configured within a device, alternatives include pre-configured devices, use of Subscription Manager - Discovery Server and companion devices.

Remote SIM Provisioning Operation – Operator Profile Selection

Should the end user wish to change operator, they can set up a contract with the new operator (4), and in turn receive a QR code from that operator. The device can scan the code to locate and download the new Profile.

In (5) the end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects (6)[2].

[1] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.

[2] With end user consent, an operator may use business rules in their Profile to restrict the ability for the end user to perform operations (4) and (5).

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at pp. 5-6.

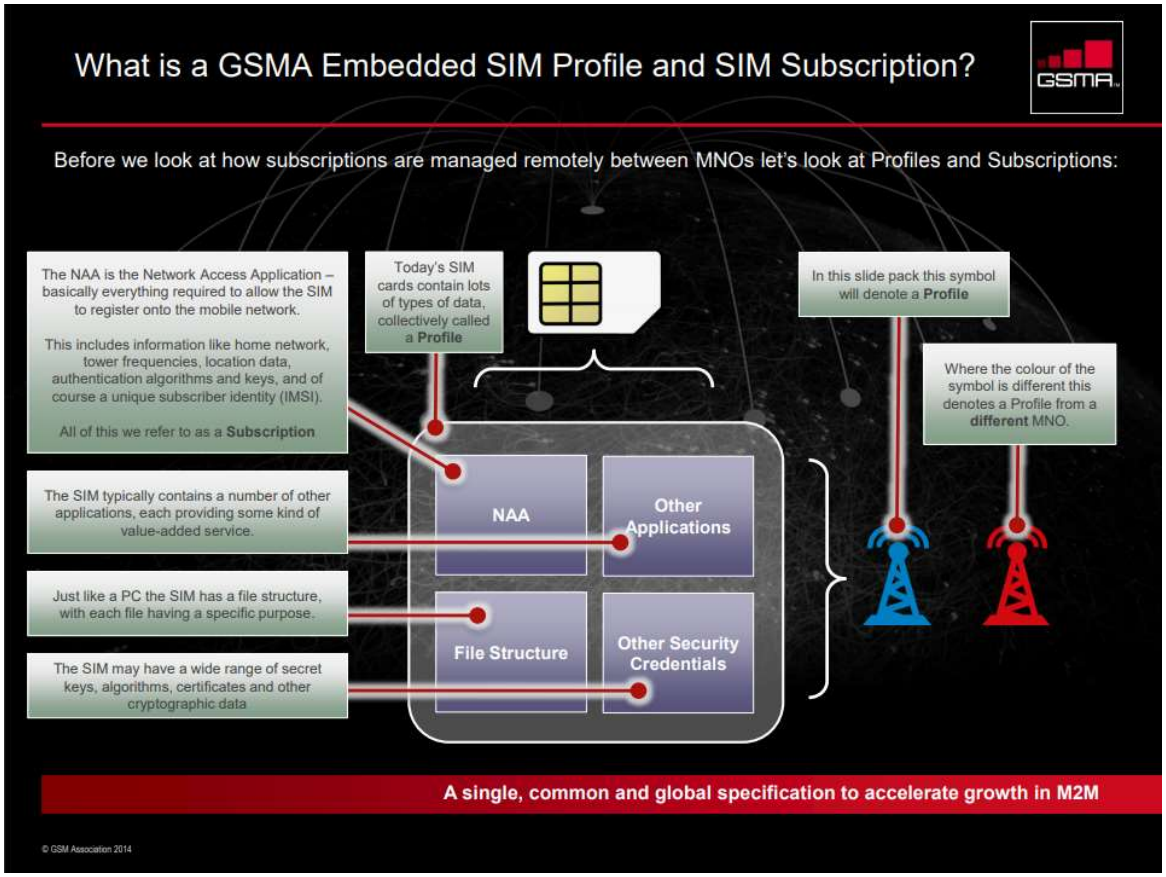
The Profile

A Profile comprises of the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The secure element in the eSIM solution is called the eUICC, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence.

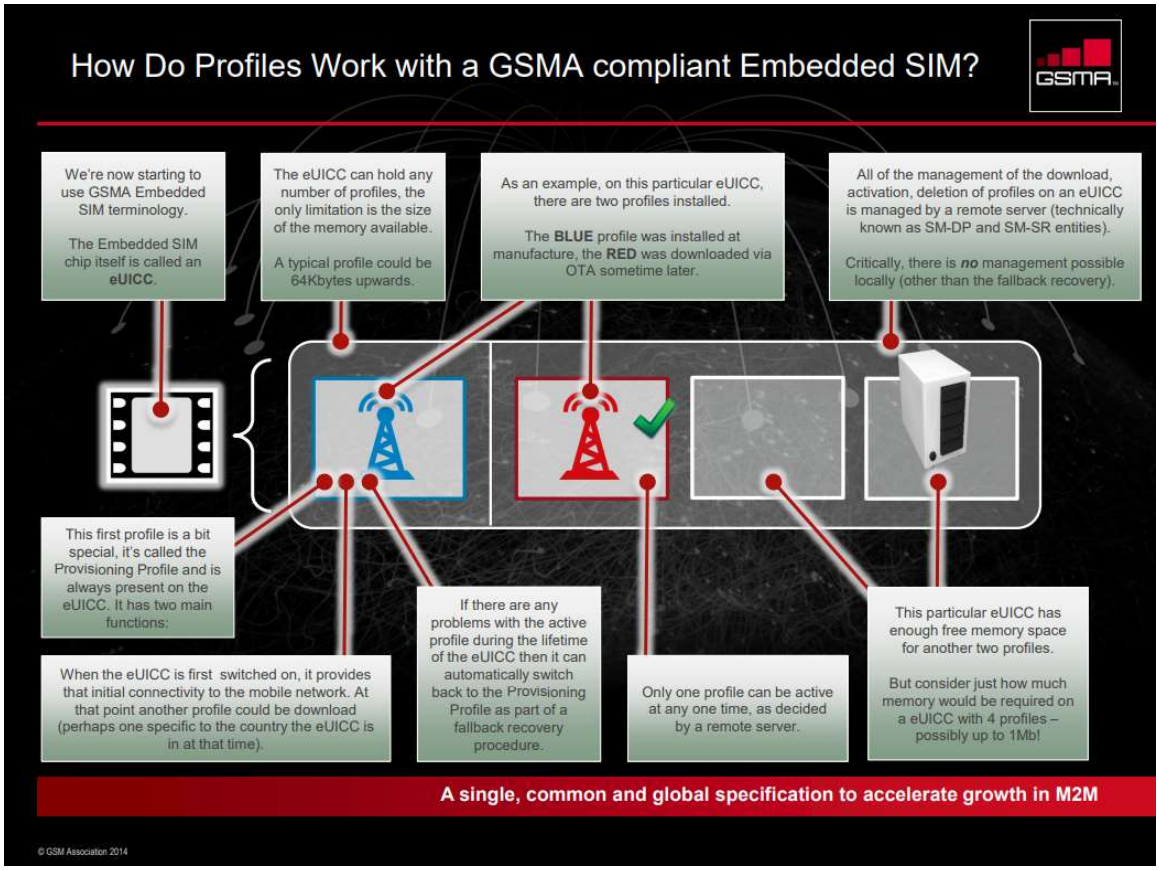
The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. The interoperable description of these Profiles is defined by the SIMAlliance[3].

[3] http://simalliance.org/euicc/euicc-technical-releases/.

See https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf at p. 6.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 23.



See https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf at p. 24.

80. On information and belief, Acer directly infringes at least claims 1, 8, and 13 of the '208 patent, and is in violation of 35 U.S.C. § 271(a) by making, using, selling, and offering to sell the Accused eSIM Products.

81. Acer's direct infringement has damaged Shingletop and caused it to suffer and continue to suffer irreparable harm and damages.

JURY DEMANDED

82. Pursuant to Federal Rule of Civil Procedure 38(b), Shingletop hereby requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

Shingletop respectfully requests this Court to enter judgment in Shingletop's favor and against Acer as follows:

a. finding that Acer has infringed one or more claims of the '156 patent under 35 U.S.C. §§ 271(a);

b. finding that Acer has infringed one or more claims of the '831 patent under 35 U.S.C. §§ 271(a);

c. finding that Acer has infringed one or more claims of the '208 patent under 35 U.S.C. §§ 271(a);

d. awarding Shingletop damages under 35 U.S.C. § 284, or otherwise permitted by law, including supplemental damages for any continued post-verdict infringement;

e. awarding Shingletop pre-judgment and post-judgment interest on the damages award and costs;

f. awarding cost of this action (including all disbursements) and attorney fees pursuant to 35 U.S.C. § 285, or as otherwise permitted by the law; and

g. awarding such other costs and further relief that the Court determines to be just and equitable.

Dated: August 16, 2021

Respectfully submitted,

/s/Raymond W. Mort, III

Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com
THE MORT LAW FIRM, PLLC
100 Congress Avenue, Suite 2000
Austin, Texas 78701
Tel/Fax: 512-865-7950

Of Counsel:
Ronald M. Daignault (*pro hac vice* to be filed)*
Chandran B. Iyer (*pro hac vice* to be filed)
Oded Burger (*pro hac vice* to be filed)*
rdaignault@daignaultiyer.com
cbiyer@daignaultiyer.com
oburger@daignaultiyer.com
DAIGNAULT IYER LLP
8618 Westwood Center Drive - Suite 150
Vienna, VA 22182

Attorneys for Plaintiff Shingletop IP LLC

*Not admitted to practice in Virginia